riverbed®

Think fast.®

Riverbed Performance Management

Dipl.-Ing. Alexander Tomík
RPM Solutions Architect

DoS, nás se to netýká?

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.

Vytvořené hranice IT architekturou

Budoucnost IT bez hranic.

1960 **2015**

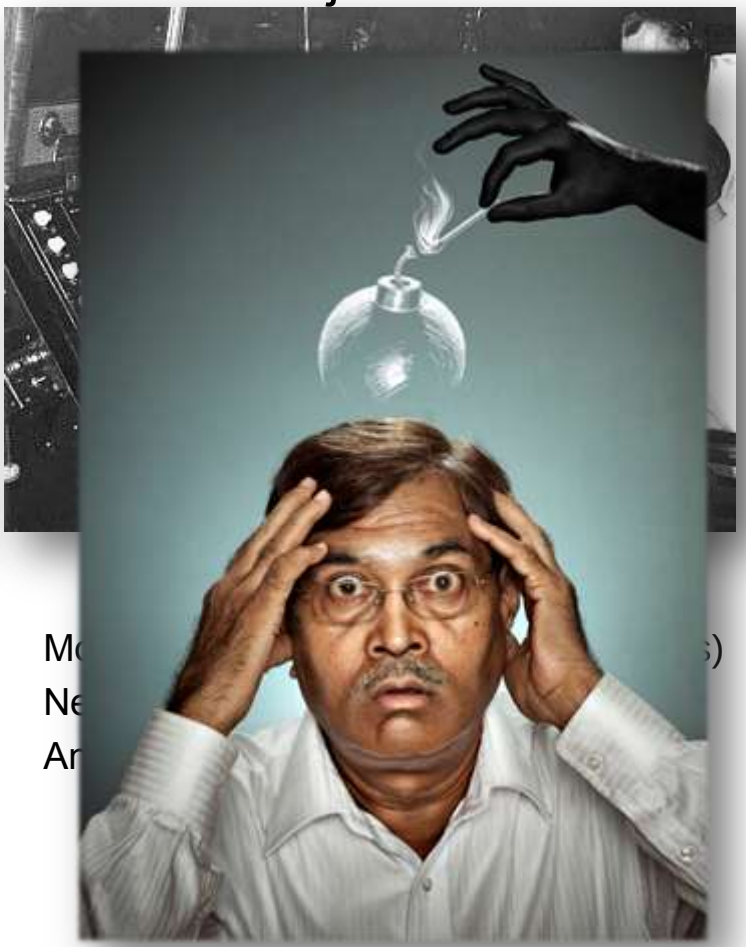
Nové úlohy, staré nástroje

riverbed

Úlohy 21. století…

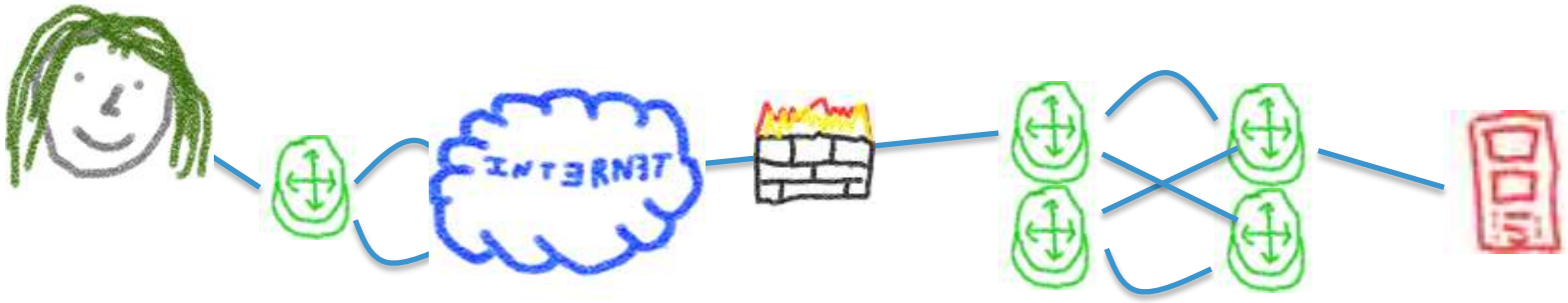
-
-
-
-
- lasu a videa

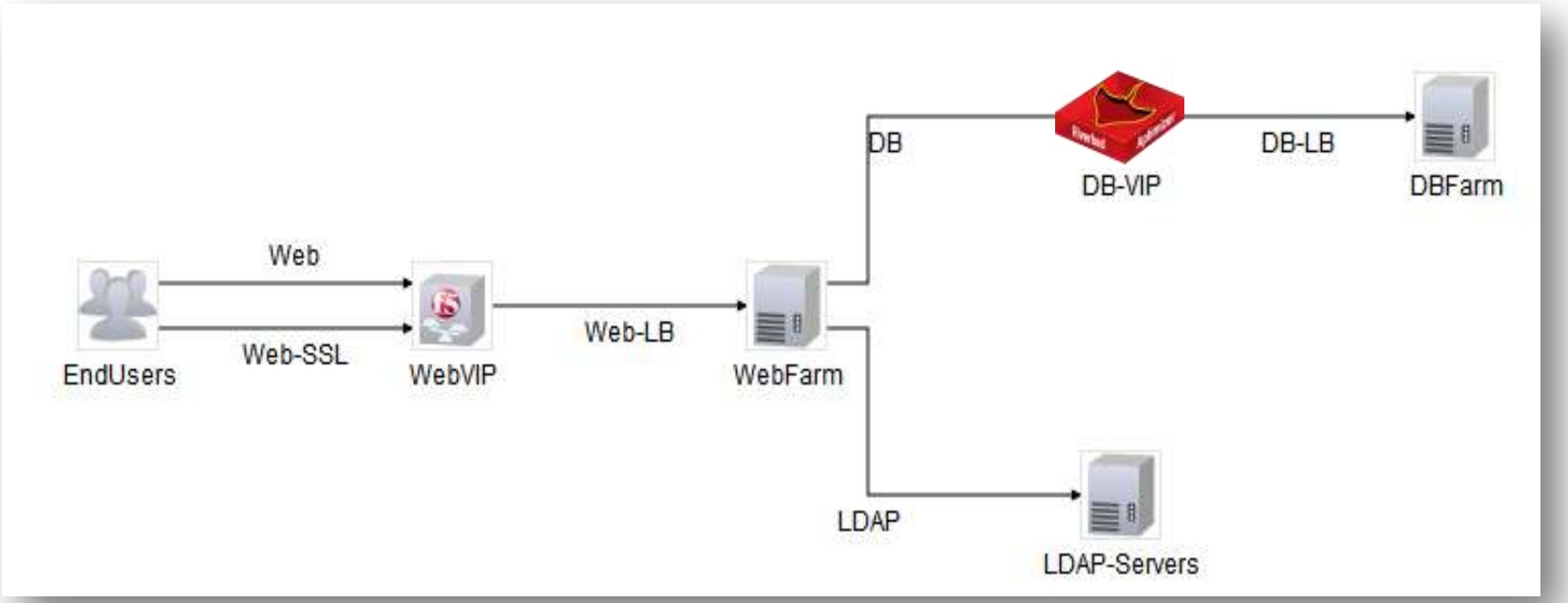
… nástroje 20. století



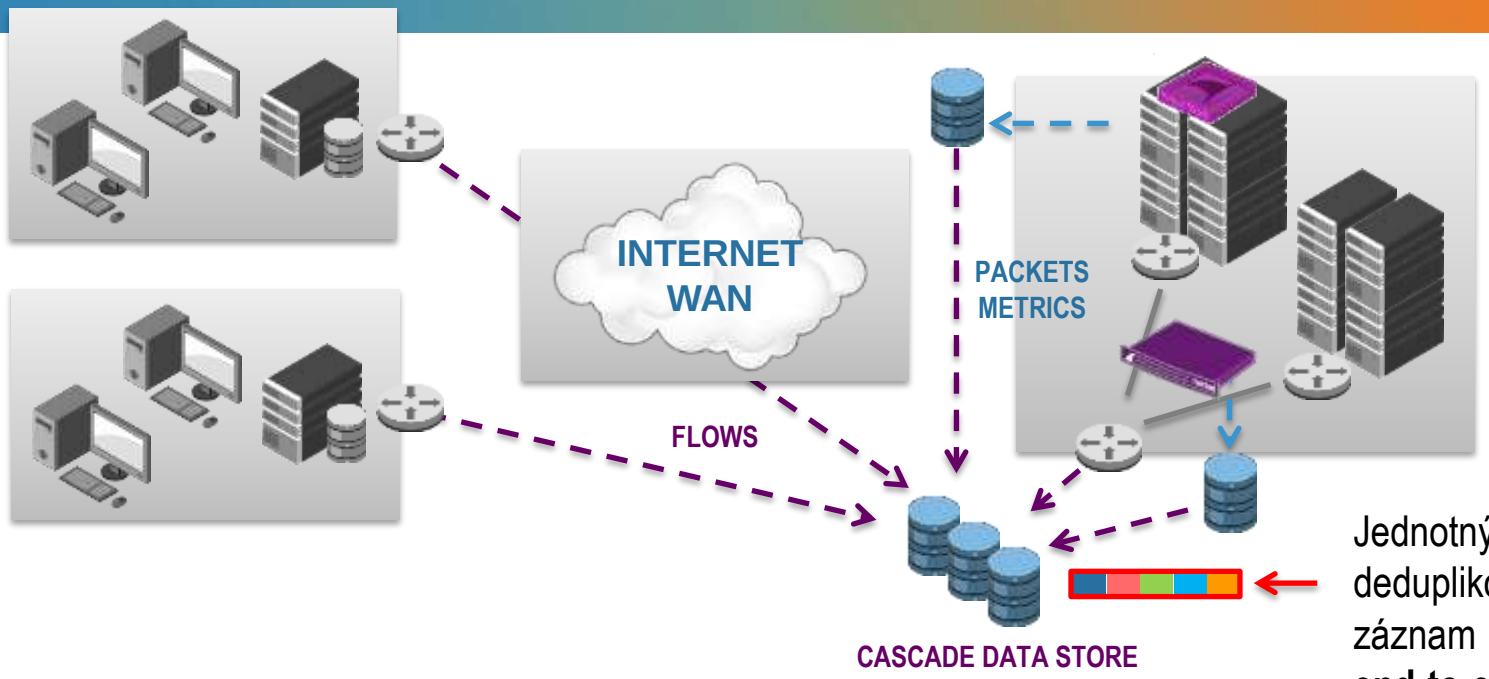
- M)
- Ne
- Ar

Znát všechny komponenty!



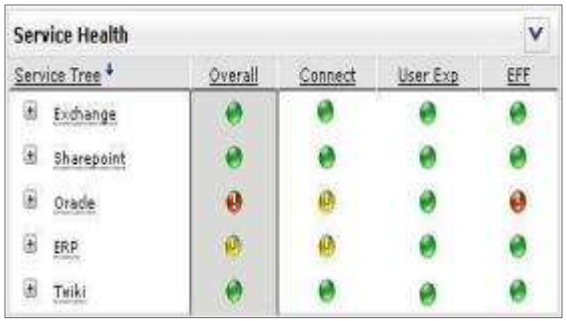


Komplexní Viditelnost s Flow & Pakety

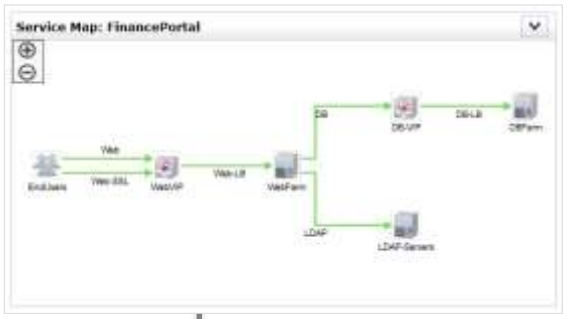


- Flow data poskytuje efektivní viditelnost end-to-end
- Packet data poskytuje podrobný přehled o výkonu aplikací - v případě potřeby

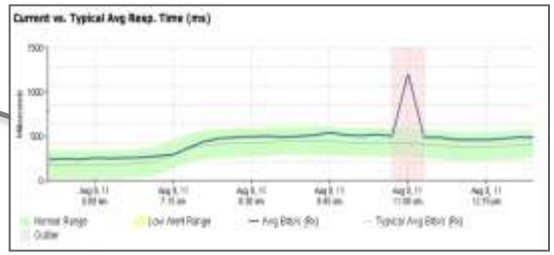
Automatizovaný monitoring



Nástroje na vytváření map a nástěnek



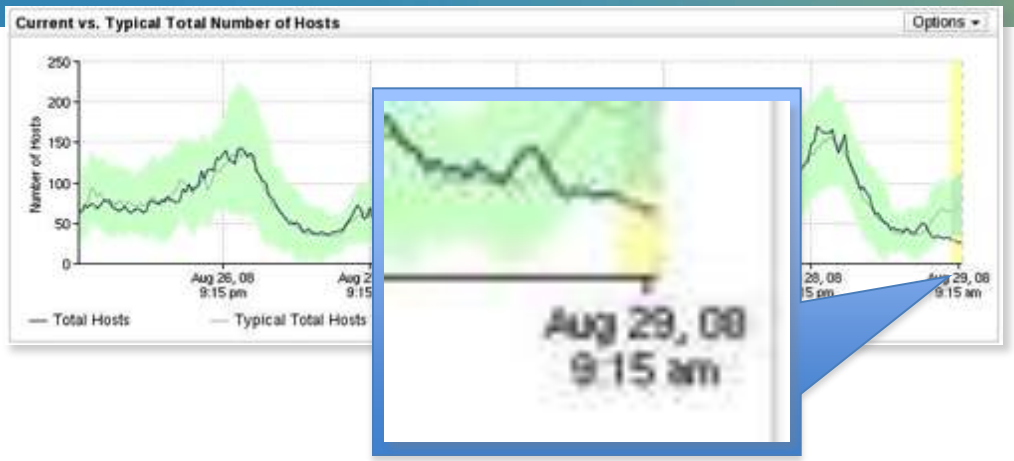
Dashboards:
Nástěnka s náhledem stavu sítě a aplikací.



Discovery:
Rychle objevit všechny komponenty aplikace.

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

Všechny metriky vaší sítě

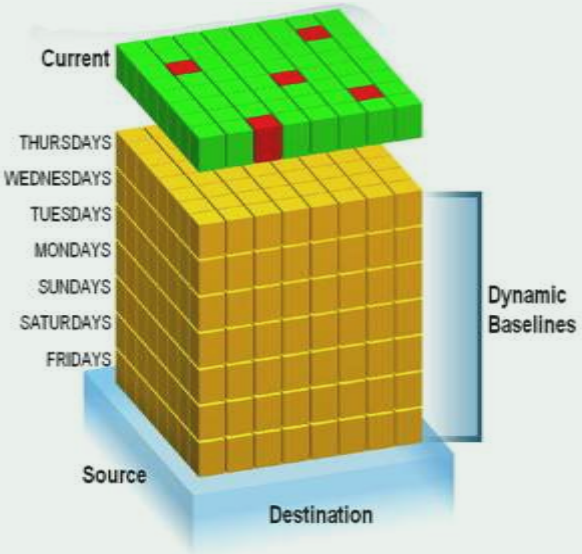


Normalizace dat umožňuje sledovat četné bezpečnostní a výkonnostní metriky ve vaší síti.

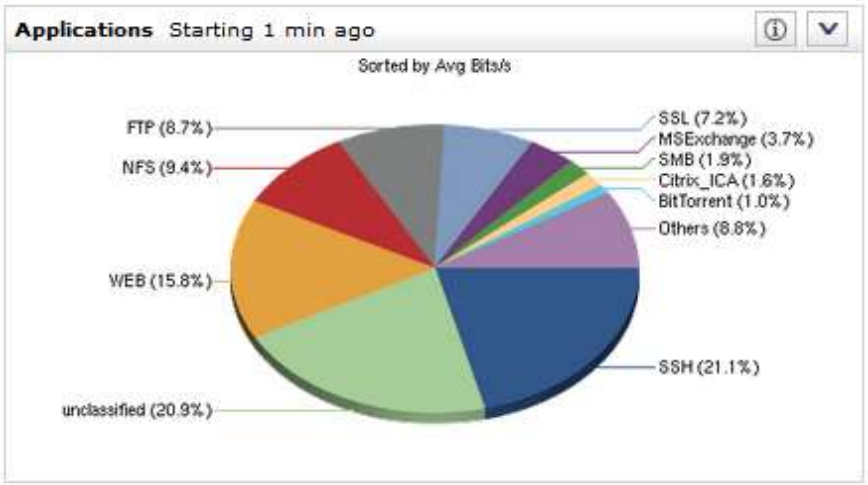
Jakmile systém vytvoří základní linii (šedá čára) můžete nastavit toleranci pro změnu (zelená cesta). Kdykoliv aktuální chování (modrá čára) překročí nakonfigurovanou toleranci, systém pošle upozornění.

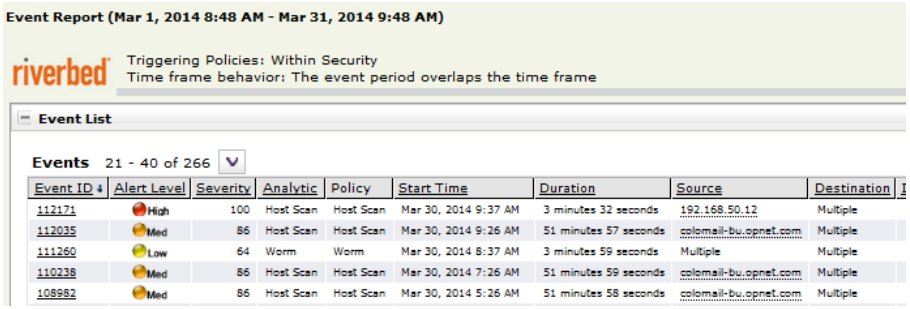
Podezřelá spojení

- *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*

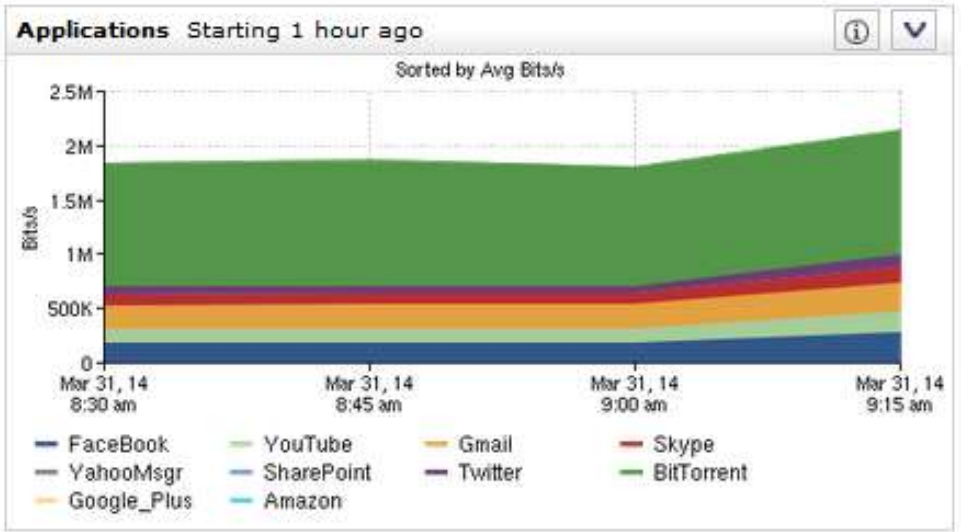


Kompletní viditelnost sítě



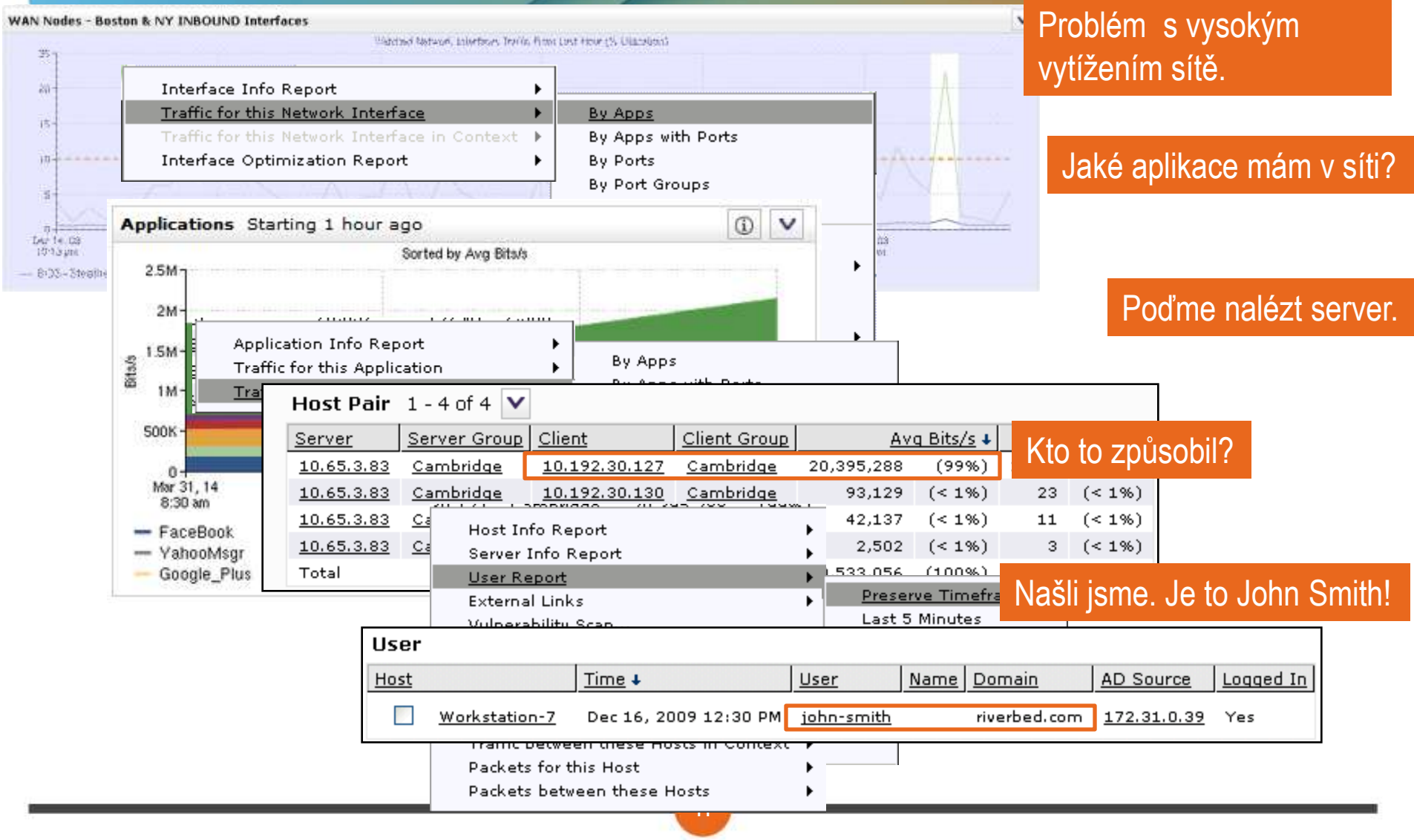


- Zjistit, které aplikace jsou v naší síti
- Rozpoznat důležité a “rekreační“ aplikace
- Získat viditelnost aplikace - kdo, kdy a odkud aplikaci využíval
- Alarmovat při podezřelém chování



ANALÝZA PROBLÉMU V SÍTI

riverbed



Problém s vysokým vytížením sítě.

Jaké aplikace mám v síti?

Poďme nalézt server.

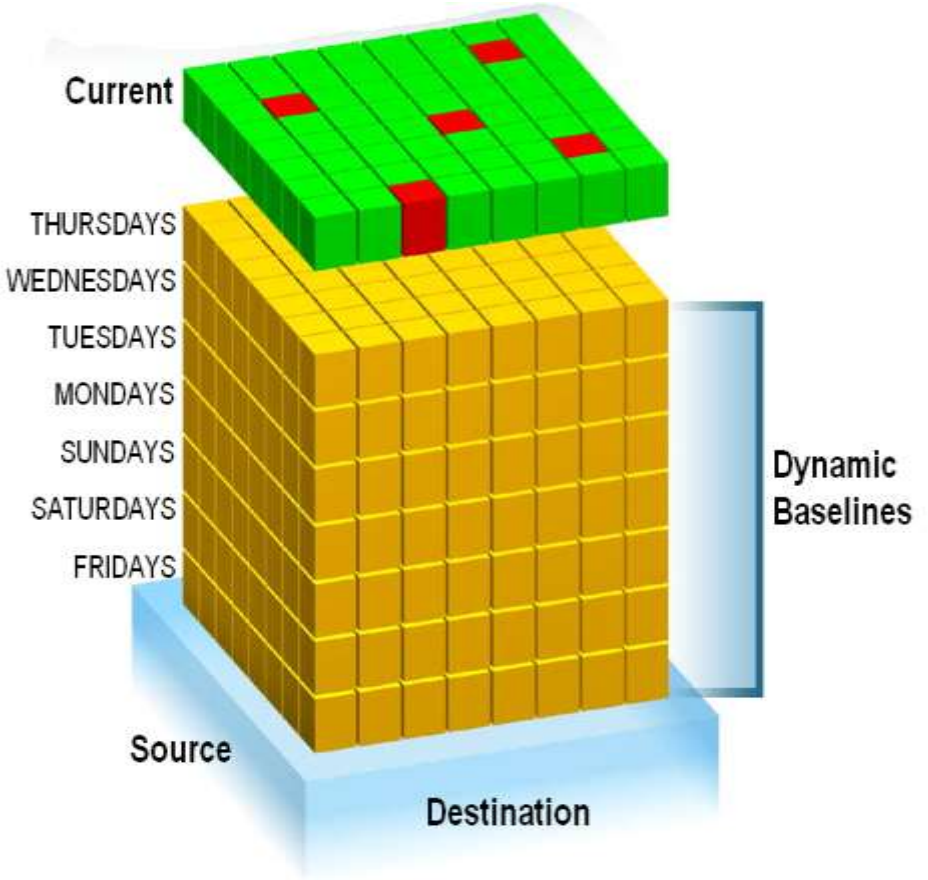
Kto to způsobil?

Našli jsme. Je to John Smith!

Co vidíme v síti....

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

- User Defined Policies



Bezpečnost pod kontrolou

riverbed

Configured Policies — 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.

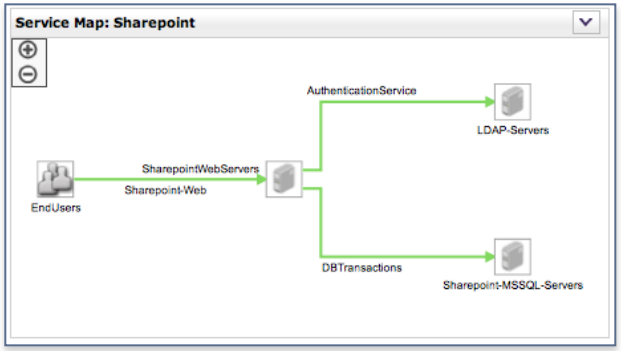
Analýza chování detekuje události založené bez podpisů.

User Defined Policies — New...

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 nepřípustné chování, jako jsou P2P, tunelování a spam činnosti.

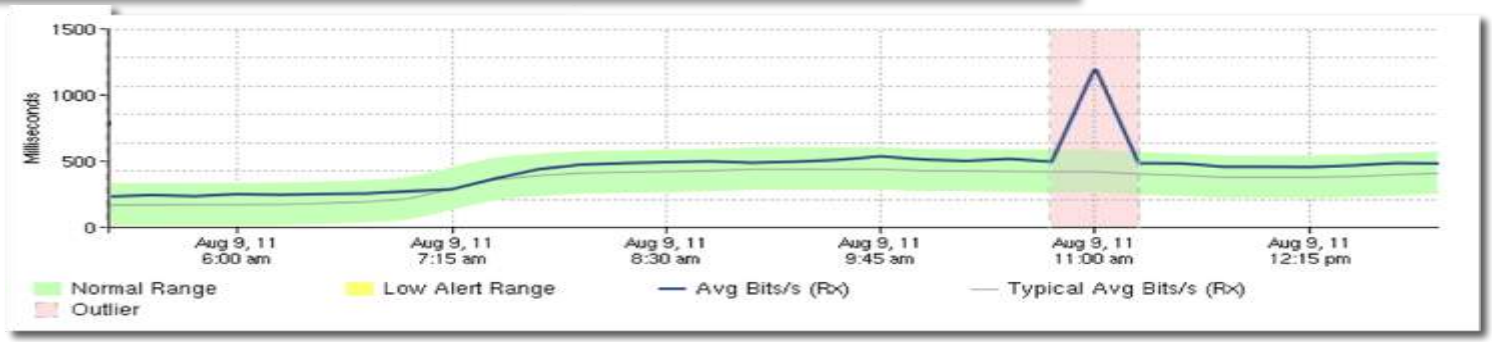
Monitorování Vašich firemních aplikací v reálném čase.

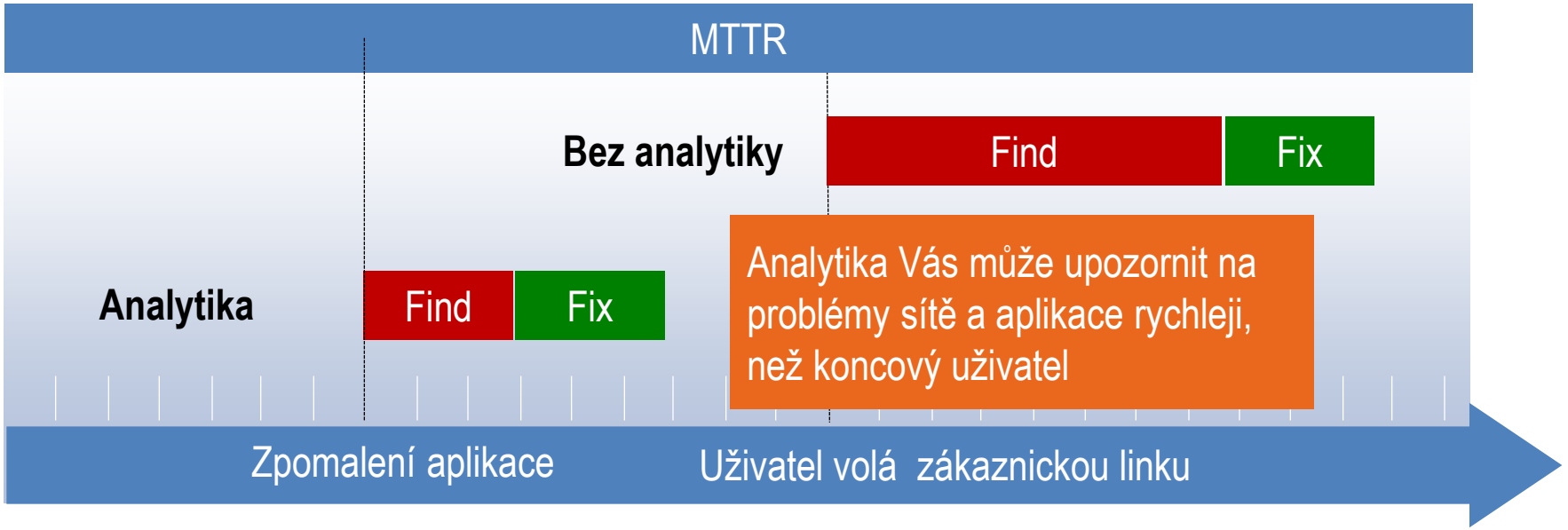


INTELIGENTNÍ MONITORING S DYNAMICKOU ANALÝZOU CHOVÁNÍ

riverbed

Doba odezvy se odchyluje od normální a spustí se výstraha.





Děkuji!

riverbed