Boosting Canada’s Cyber Immune System for Internet Health

Matt Broda
Technical Fellow - Security

November 2017
Cyber security risk on the rise

Enterprises are more vulnerable than ever.

- 99 days median time to discover
- 40% increase in number of breaches in 2016
- $255 cost per stolen data record (Canada)
- Limited situational awareness
- Growing attack surface
- 202.5 Gbps largest DDoS attack recorded by Bell
- Sophisticated adversaries
- Security arms race
- 16+ hours longest DDoS attack
- $5B losses due to ransomware - 15 fold increase from 2 years ago
Its time to think differently…

Let go of the island mentality - **expand your defense.**

Cyber security is a **business risk** challenge, look for simple, sustainable solutions.

Minimize your blind spots - **awareness** enables effective action.

Don’t underestimate your **adversary** - they follow a clear business objective and leverage broad **supply chain** to achieve.

Avoid single points of failure - **take defense-in-depth.**

How healthly is your cyber immune system?
Leverage your partners to boost your defense

<table>
<thead>
<tr>
<th>Cloud &amp; Mobile</th>
<th>Existing security models</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer</td>
<td>CPE Security</td>
<td>Cloud Security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performance</th>
<th>Agility</th>
<th>Scalability</th>
<th>Cost per Branch</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
Diagnostics - Cyber threat analytics

25K+
Unique indicators generated monthly

65+ days
Malicious entities identified in advance of community

92% accuracy
Improving Machine Learning accuracy
Inoculation - Network protection as a service

- Secure Internet Access
- Data Centre Protection
- Road-warrior Remote Access
- 3rd Party
- LTE / 5G
- Secure Mobile Device Access
- Secure IoT Access
- LTE / 5G WiFi
- Dedicated cloud access

Cyber Threat Analytics
Security Operations Center
- Application Protocol Anomaly Detection
- Content Inspection and Sandboxing
- Cloud Access Security Broker
- Client Access Always-On VPN
- Encryption / Decryption
- Data Leak Prevention
- Site-to-Site VPN
- DDoS Protection
Conclusion

Enterprise cyber security risks are on the rise.

Think of cyber security as a business problem - optimize the approach and maximize the cyber security budget.

Carriers are gateways to the Internet and have a unique role to play in community-based defense-in-depth.
Thank you

Matt Broda
Matt.broda@bell.ca
(613) 785-8224