

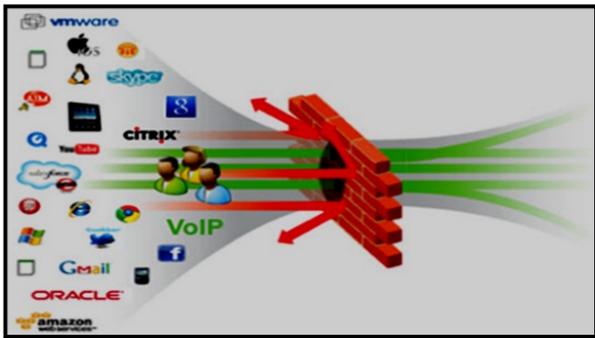
Zero-trust Implementation with Cisco Tetration Analytics

Trying to wrap your mind around Micro-Segmentation or Nano-Segmentation? Want to know the effect of a Firewall rule change prior to implementing in production? Implementing tighter security controls brings its own risks of breaking something in production. Cisco's Tetration Analytics has the capability to do a logical test against historical flow data on what a security implementation would do and its effect on production network flows. Tetration Analytics dramatically simplifies your zero-trust implementations. It provides visibility into everything in your data center in real time by using behavior-based application insight and machine learning to build dynamic policy models.

<http://cs.co/90038j47Z>



The more you see, the better you can protect! - Cisco Application Visibility and Control (AVC)

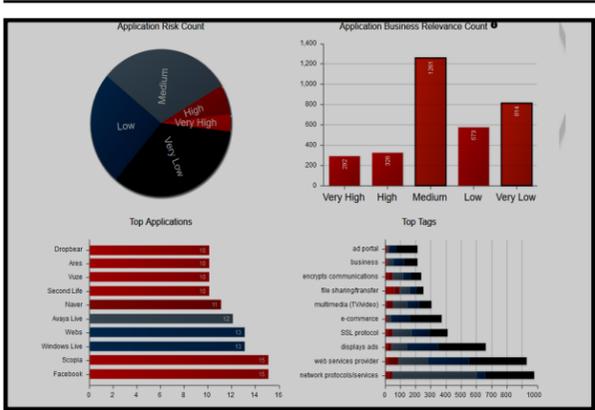


Cisco AVC: <http://cs.co/90088jAq4>

It's no secret that we live in an application loaded world, be it corporate or social. Applications have evolved to be highly dynamic and multifaceted, blurring the line between business applications and personal ones, increasing company's exposure to Internet-based threats. Visibility into well-known port numbers are a thing of the past. These days, more applications are using HTTP as transport mechanism.

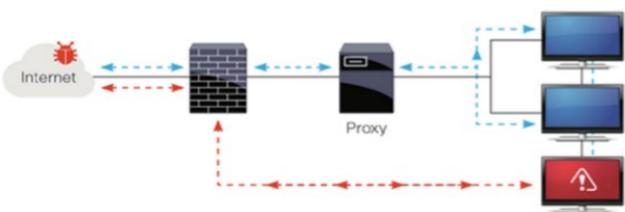
Deeper visibility has to be enforced for Port hopping applications, peer-to-peer apps to provide effective security controls. Base license of Cisco NGFW includes AVC functionality making it easier to identify applications, micro applications and enforce policy. As an example, you may allow Facebook for business use, but disable other components such as Facebook Games. The latest AVC data base supports 4000 applications by default and over 180,000 micro applications. Cisco OpenAppID framework allows you to extend AVC to any proprietary and custom apps.

Check out tool to look up application coverage on NGFW: <http://appcoverage.cisco.com/>



See and detect more threats. Assess your network visibility and security using Cisco Stealthwatch for free!

Cisco is offering a free Stealthwatch visibility assessment that will help organizations evaluate their internal network visibility and security posture. After the 14 day assessment, a detailed assessment report identifying areas of risk will be provided. Few of the key topics in assessment includes Behavior analysis, Proxy violation, Rouge servers, DNS risk, Internal hosts being controlled remotely, Data exfiltration etc.



<http://cs.co/90038jfdU>

Compare Endpoint Security Solutions

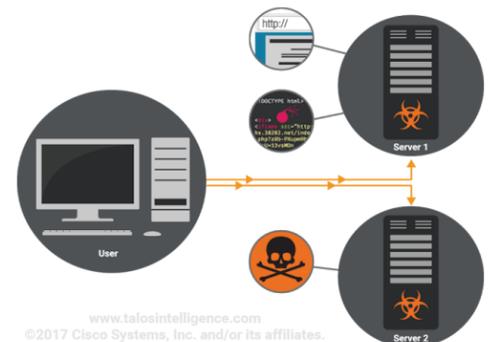
	Cisco AMP for Endpoints	Carbon Black Endpoint Security	CrowdStrike Falcon	CylancePROTECT
Detection				
Number of integrated detection techniques	14	4	4	1
Continuous analysis and retrospective detection	✓	Limited	✓	✓
Device trajectory	Continuous	✓	✗	Limited
Detection measures	Multiple	Multiple	Multiple	Single
Dynamic file analysis	Threat Grid	✗	✗	✗
File analysis deployment model	Both	✗	✗	✗
API support	✓	✓	✓	Daily reports
File trajectory	✓	Limited	Limited	✗

Read complete report: <http://cs.co/90048jfpo>

Threat Spotlight: Sundown, an exploit kit in transition.

Sundown, an exploit kit that many considered relatively unsophisticated a few months ago is gradually evolving into a substantial threat. The exploit kit landscape has been struggling to find its footing since the major players have left. Sundown is one of the few exploit kits adding any new exploits to their arsenal, same time they consistently steal exploits and technologies from other people and competitors

<http://cs.co/90008jAJ2>



Webinars: Register Now

- [April 14: What's New with AMP](#)
- [April 21: Cisco Umbrella](#)

For more information on Cisco Security solutions and products, please contact your **Cisco Account Manager**

Suggestions/comments on this newsletter contact Joby James at joby@cisco.com

