sandvine®

Intelligent Broadband Networks

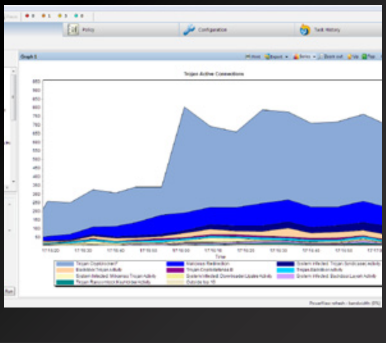
Protect your network and subscribers from online threats.

Security is best achieved with a layered approach, and perhaps no layer is as important as the network itself.

But only a solution engineered specifically to secure the untrusted environment of the Internet can provide effective defense against today's threats.

Whether your motivation is to protect your subscribers, your network, or your reputation – or perhaps even respond to regulatory pressures – we've got you, and your network, covered.

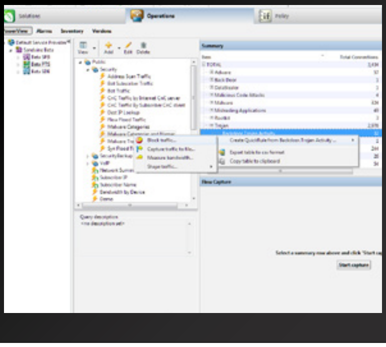
Do more, with Sandvine.



Real-Time Visibility

Our Control Center interface provides you with vital real-time visibility into active threats, and can be used to trigger alarms or automatic mitigation.

For audit purposes and historic reporting, security events are logged and can be viewed in our Network Demographics interface or fed into other systems for ongoing operational intelligence.

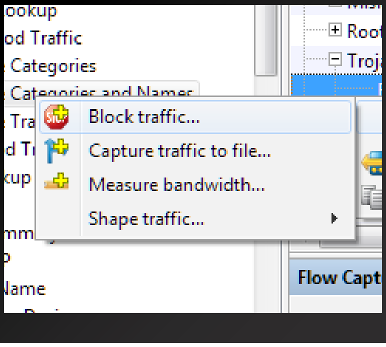


Advanced Detection

We provide unmatched threat detection through a combination of behavioral signatures and data-feeds, so you can rest easy.

The behavioral signatures – which include multi-factor analysis and configurable sampling thresholds – provide zero-day detection.

Data-feeds provide detection of specific forms of malware and dangerous or illegal content.



Effective Defense

Once threats are detected, a range of actions can be taken, including: flow rate-limit, BGP flowspec, mark, divert, tee to file, and – of course - block.

These actions can be applied with varying degrees of automation, to fit your operational model.

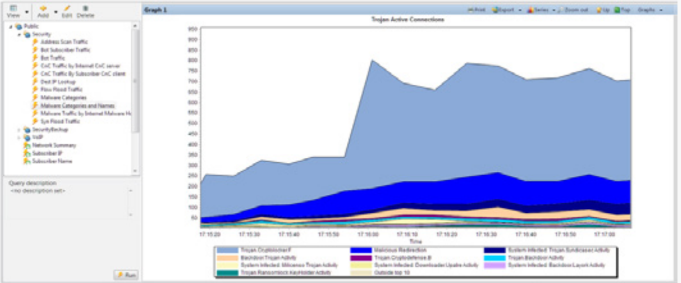
Plus, you can even take measures to engage with subscribers to notify them of infections.

Visit www.sandvine.com

EXAMPLE USE CASES

Malicious Traffic Monitoring

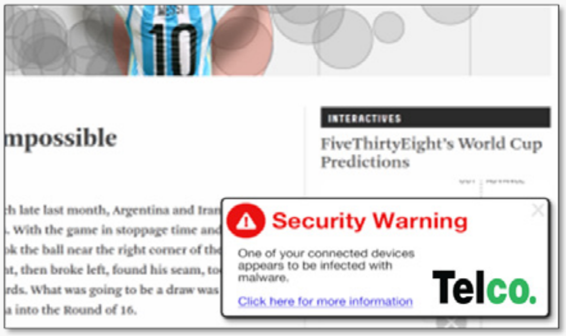
Monitor real-time malicious traffic activity by location, subscriber, and network-wide.



Sandvine Control Center displaying active connections to malicious traffic categories in real-time through PowerView

Warn and Protect Subscribers

Detect devices generating malicious traffic or that are connected to known threats and notify users to take corrective actions.



mpossible

FiveThirtyEight's World Cup Predictions

h late last month, Argentina and Iran
. With the game in stoppage time and
k the ball near the right corner of the
t, then broke left, found his seam, to
rds. What was going to be a draw was
a into the Round of 16.

Security Warning

One of your connected devices appears to be infected with malware.

Click here for more information

Telco.

Real-time security notifications with Sandvine OutReach

Botnet Detection and Disruption

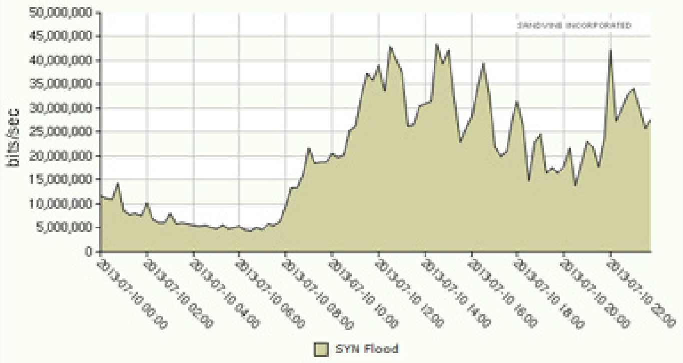
Detect subscribers who have fallen prey to botnet infection and disrupt botnet operations.

Web Filtering Services

Hassle-free, network-wide URL and web filtering based on topical categories.

DoS/DDoS Protection

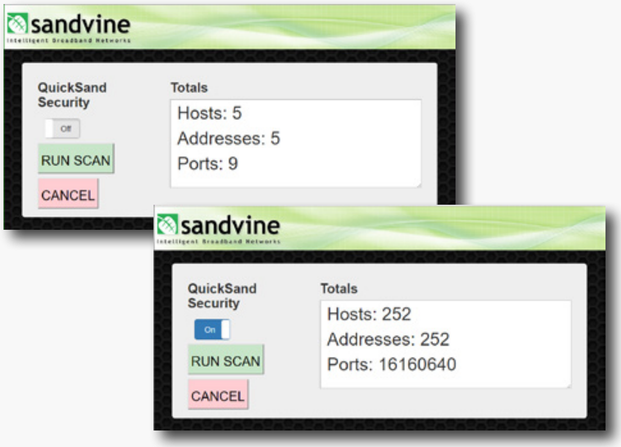
Leverages Sandvine's subscriber awareness for visibility into each subscriber flow to not only detect and prevent large scale, volumetric DDoS attacks, but surgical attacks that aim to exhaust the resources of a specific server as well.



SYN flood activity report in Network Demographics

Network Threat Deception

Deception and decoy techniques that work at carrier-grade scale and materially change attack economies.


sandvine
Intelligent Broadband Networks
Off
RUN SCAN
CANCEL
sandvine
Intelligent Broadband Networks
On
RUN SCAN
CANCEL

QuickSand Security

Totals

Hosts: 5
Addresses: 5
Ports: 9

QuickSand Security

Totals

Hosts: 252
Addresses: 252
Ports: 16160640

Sandvine QuickSand: network scale tarpitting demonstration

Visit www.sandvine.com

Sandvine Incorporated ULC
408 Albert St. Waterloo, Ontario Canada N2L 3V3
+1 519 880 2600 | www.sandvine.com