Seculert

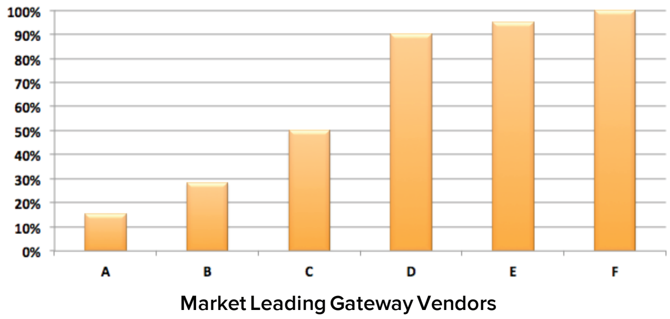
ArcSight, BlueCoat, Fortigate, LogLogic, LogRhythm, McAfee, Palo Alto, QRadar, Splunk, Websense, ZScaler

Research Finds Critical Gaps in Gateway Solutions

Fast Facts

- ♦ **788,000 client devices**
- ♦ **62 billion total communications**
- ♦ **6 Gateway Vendors** – BlueCoat, Fortigate, McAfee Web Gateway, Palo Alto, Websense, ZScaler
- ♦ **6 SIEM Products** – ArcSight, LogLogic, LogRhythm, McAfee SIEM, Splunk, QRadar
- ♦ **Duration 3 Months**

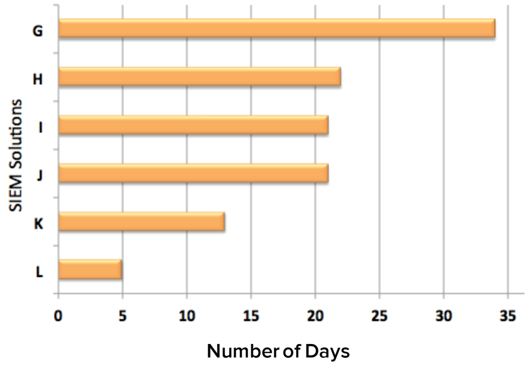
PERCENTAGE OF DEVICES ALLOWED TO COMMUNICATE OUT



Key Findings

- ♦ The very best performing secure gateway allowed 15% of the infected devices to communicate out to the perpetrator’s command and control servers
- ♦ Three of the six gateways observed allowed 90% or more of the infected devices to send communications to the malware’s perpetrators
- ♦ Roughly 2% of all devices examined were infected, and every examined environment contained infected devices able to communicate out
- ♦ Approximately 36% of all infected devices were allowed to communicate out to perpetrators; 13% of malicious communication attempts were successful
- ♦ Using just the secure web gateway products, it took an average of 17 days from the first malicious communication until a breach was contained
- ♦ Prior to deploying Seculert, it took enterprises using one of the leading SIEM products an average of up to 5 weeks to contain a breach. The desired SLA to contain a breach is typically 2-3 days

DAYS TO CONTAIN



Automated Breach Analytics Platform

Seculert’s automated breach analytics platform protects global enterprises from the effects of targeted malware attacks. The Seculert platform drives the network egress monitoring service; which fully automates the breach detection process. Seculert provides a compensating control to protect key IT infrastructure even when the primary prevention systems fail. Seculert delivers malware infection reports that are 100% verified as “true positives.” The Seculert Platform uses a combination of Big Data analytics, machine learning, and external context to generate unique malware profiles that are used to identify new infections. The Seculert Platform significantly improves malware detection while providing unprecedented visibility on overall security system performance. Seculert requires no hardware or software, no agents, and no changes to current security workflow processes.

United States

2880 Lakeside Drive, #228
Santa Clara, CA 95054
Tel: +1 408 560 3400

Israel

6 Efal Street, P.O. Box 3970
Petach Tikvah, IL 4952801
Tel: +972 3 919 3366

Free Report Download

Visit seculert.com or scan
the code to downloadthe full
“State of Perimeter Security” report.