REPORT

Perimeter Security Defenses

State of Perimeter Security Defenses, Time to Think Different?

Table of Contents

Introduction

According to Gartner, Inc., businesses spent over $71 billion on information security in 2014, yet that investment is failing to stop the nearly $400 billion global loss as a result of cybercrime and the advanced targeted attacks plaguing enterprises.

For years, cyber-security innovation and investment have been directed towards technologies that aim to prevent or block incoming attacks, but as the volume and sophistication of malware continues to grow exponentially, staying ahead of the latest attack has become a losing game for security teams. Prevention-focused security strategies are now known to fail on a regular basis. Enterprises that rely only on prevention-focused perimeter security tools like next generation firewalls, IPS, and secure web gateways are positioning themselves in the crosshairs of cybercriminals and other adversaries capable of penetrating modern perimeter security defenses with startling ease. While useful, these prevention solutions alone cannot protect organizations in the current threat landscape.

Increasingly, CISOs and CIOs are aware that their organization has been breached, and want to understand what devices are infected and with what malware. CISOs now need to begin thinking differently about their entire security strategy and complement their prevention architectures with automated breach detection solutions.

Seculert examined a subset of its installed base environments, in the last quarter of 2014, to determine whether existing gateway tools were allowing internal devices to be infected and communicate malicious traffic outside of the organization. The company also examined how long it took those organizations to contain the breach once it was identified. Even in those enterprises that had comprehensive and well-run perimeter defense systems in place (including a secure web gateway and/or next generation firewall, an IPS, endpoint protection and a SIEM), the rate of failure was material.

The gateway solutions observed included those from BlueCoat, Fortinet, McAfee, Palo Alto Networks, Websense, and ZScaler. SIEM products observed included HP ArcSight, IBM® Security QRadar® SIEM, Splunk, RSA Security Analytics, TIBCO LogLogic®, LogRythm, and McAfee Enterprise Security Manager. The environments studied included 788,000 client devices that generated nearly 62 billion total communications based on Fortune 2000 companies in North America during Q4 of 2014.

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%+ (ninety plus percent) of the infected devices to send communications to the malware's perpetrators (Figure 2).
- Roughly 2% (two percent) of all devices examined were infected, and every environment examined contained infected devices that were allowed to communicate out.
- Approximately 36% of all infected devices were allowed to communicate out to their perpetrators, and 13% of all attempted malicious communication succeeded.
- Of the 62 billion total communications observed, nearly 3 million attempted malicious outbound communications were generated from infected devices. Of these attempted communications, roughly 13% successfully reached the perpetrators command and control infrastructure.
- On average, it took 17 days from the first malicious communication until a breach was contained. Also, it took Seculert customers, using one of the SIEM products, an average of up to five weeks to contain a breach (Figure 3). The desired SLA by Seculert customers to contain a breach is 2-3 days.

Secure Gateway Vendor	Total Devices Monitored	Daily Average Percentage of Infected Devices	Percentage of Infected Devices Allowed to Communicate	Total Communications (billions)	Attempted Malicious Outbound Communications Observed	Malicious Communications Allowed Out	Percentage of Malicious Communications Allowed Out
1	496,231	1.50%	16%	42.5	668,669	66,367	10%
2	111,335	3.30%	28%	11.0	1,762,548	81,249	5%
3	124,838	1.60%	95%	1.2	509,000	225,759	44%
4	9,806	1.10%	90%	1.1	20,552	6,334	31%
5	6,314	6.30%	100%	0.9	3,013	2,741	91%
6	39,692	5.00%	50%	5.2	2,679	636	24%
Total	**788,216**	**2.00%**	**35.90%**	**61.9**	**2,966,461**	**383,086**	**12.90%**

Figure 1

Percentage of Infected Devices Allowed to Communicate Out

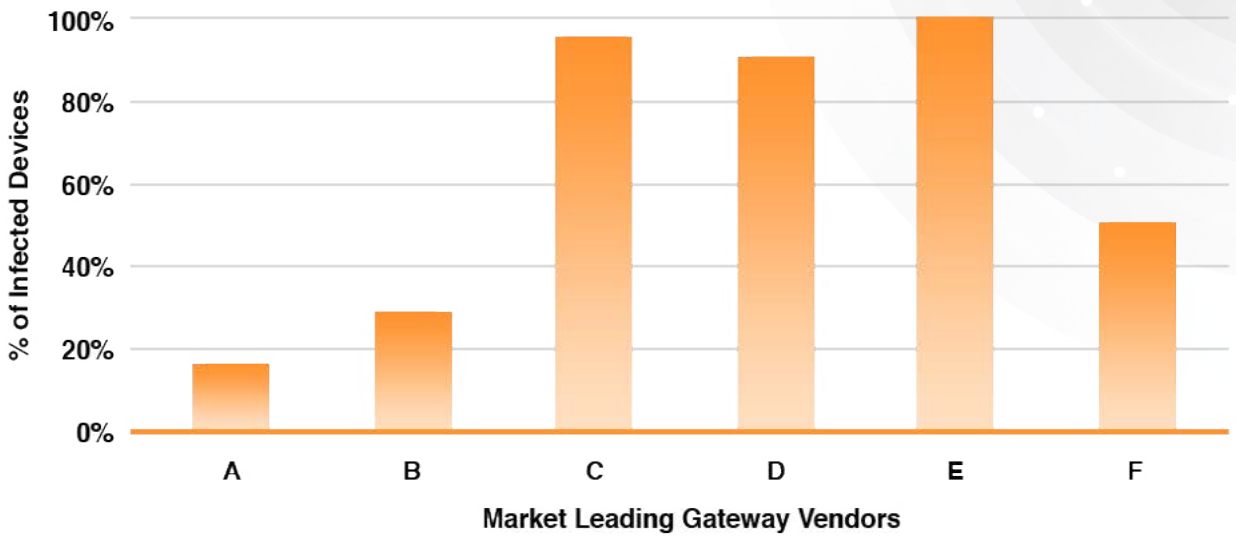

Figure 2

Days to Contain

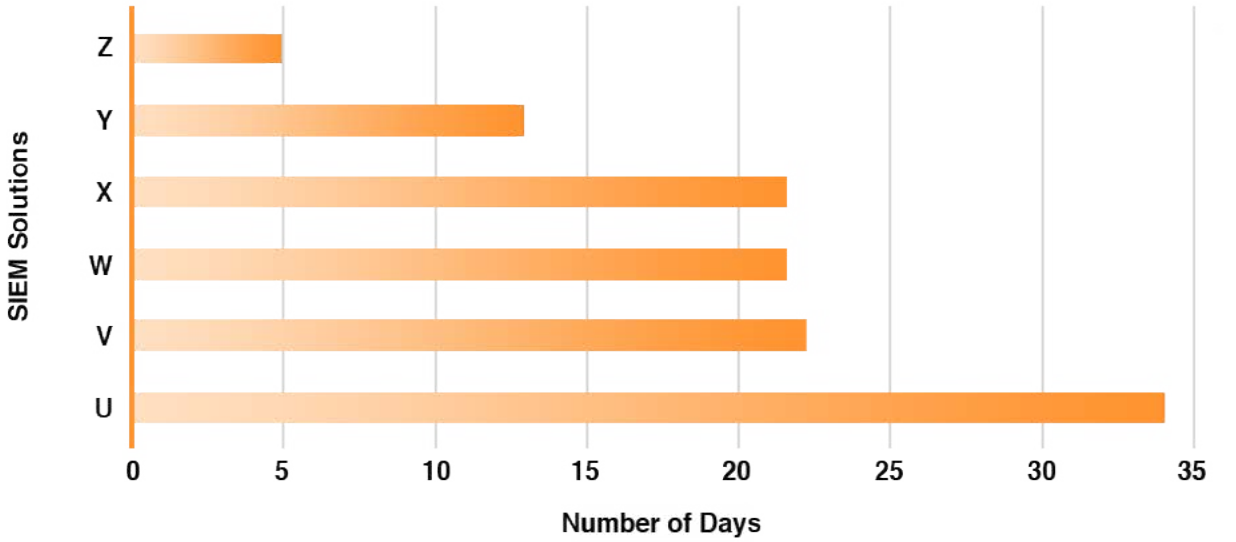

Figure 3

A comprehensive analysis for the reasons these solutions fail is beyond the scope of this report. However, the two pre-eminent drivers of these results is that (1) prevention systems are forced to do their job in near-real time and (2) depend upon manual search, correlation, and discovery processes that are labor intensive. Many cyber-criminal gangs have found highly effective ways to leverage these limitations and defeat current prevention and correlation technologies.

Implications

CISOs now need to thinking differently about their entire security strategy and rely more on automated detection and compensation control solutions. As shown, prevention technologies are not failsafe. While abandoning prevention and correlation technologies is not feasible, expectations around the role they play must change.

The term “defense in depth” has been used to mean many different things as the IT security industry has evolved. What the last year has demonstrated is that it must now include the somewhat counterintuitive notion that all modern, well-run prevention systems will inevitably fail and that having “in-depth” protection means having the plan and the ability to respond when they do.

Discover what your existing security systems have missed. Contact Seculert today by phone at +1-855-732-8537 or by email at info@seculert.com to set up a demo with one of our security experts.

Cloud-based, Automated Breach Detection

Seculert fills the gaps in existing advanced threat defenses by focusing on the blind spots found in breach prevention systems. In an era when infection is inevitable and adequate resources to find and remediate threats are limited, the Seculert Platform identifies new threats with unprecedented speed and precision. Leveraging its Big Data analytics as a service, botnet interception, and elastic sandbox functionality, Seculert provides superior detection while driving down the cost and time it takes to remediate. For more information on Seculert, visit www.seculert.com.

Contact Us

Toll Free: (US/Canada): +1-855-732-8537
Tel (UK): +44-203-355-6444
Tel (other): +972-3-919-3366
Email: info@seculet.com
www.seculert.com