In the face of today's hyper-aggressive cyber-security landscape it's critical that organizations think differently. Too often organizations continue to invest in areas that are becoming less effective as malware actors have faced the typical formula of security infrastructure for years. Clearly firewalls, AV and the like are not sufficient to address all of an organizations security vulnerabilities. Below is a compelling matrix defined by SANS Institute illustrating security spending and the calculated effectiveness of the investment. Access Control is defined in the top position and is often an area that is overlooked by many organizations.

The "Trusted LAN" is too often overlooked as a critical area to secure. Given the proliferation of new devices and device types that have joined networks over the last five years including, virtual endpoints, BYOD devices and IoT assets, IT's ability to identify and control this infrastructure has been significantly diminished. Clearly there is a compelling need to restore the "Trusted LAN".

Technology Spending and Effectiveness

Technology Options	Spending Rank	Spending	Big Win Rank	Big Wins	Effective Rank	Effective
Access and authentication	1	88.1%	1	30.6%	1	45.5%
Advanced malware prevention (IPS/UTM, other)	2	80.2%	2	28.9%	3	42.1%
SIEM	11	57.9%	3	25.6%	14T	26.4%
Vulnerability Management	8	64.3%	4	24.8%	9	31.4%
Continuous Monitoring	5	69.0%	5	24.0%	6T	36.4%
Network traffic visibility (monitoring, decryptors, etc.)	7	66.7%	6	22.3%	7	35.5%
Data protection (DLP)/Encryption	4T	69.8%	7T	20.7%	8T	33.1%
Analytics (including visualization)	9T	59.5%	7T	20.7%	15T	24.0%
Incident response tools	12	54.0%	8T	18.2%	6T	36.4%
Log management	6	67.5%	8T	16.5%	5	38.0%
Mobile device management	10	58.7%	9	16.5%	10	30.6%
Security device management	13T	53.2%	10	15.7%	12	28.9%
Wireless security	4T	69.8%	11T	14.9%	4	41.3%
Cyberthreat intelligence services	15	47.6%	11T	14.9%	15T	24.0%
Endpoint security (other than BYOD protections)	3	74.6%	12	14.0%	2	43.8%
Application security - secure development	14T	51.6%	13T	11.6%	11	29.8%
DDoS protection	13T	53.2%	13T	11.6%	14T	26.4%
BYOD security (MDM/NAC, etc.)	9T	59.5%	14	10.7%	8T	33.1%
Application security (life-cycle management or monitoring)	14T	51.6%	15	9.1%	13T	27.3%
Security intelligence platform	16	35.7%	16	7.4%	13T	27.3%
Embedded device security or monitoring (IoT)	17	27.8%	17	4.1%	16	19.0%

SANS Institute 2016 IT Security Spending Trends

Here are key 7 considerations that organizations should take into account in order to ensure comprehensive security is in place and to prepare for GDPR and Privacy Shield requirements:

1. Keep doing what's already been identified as prescriptive since security is a critical business imperative. Backups, Encryption, Firewalls, AV, etc. These are effective components, but not sufficient to address all of an organizations vulnerabilities. In 2016 organizations invested nearly $100B in security. Unfortunately, cybercrime extracted $600B from the global economy last year. That number is expected to rise to $6T by 2021. (http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016) Is your business expected to grow 10X to keep up with this negative revenue forecast?

   *Cybercrime damages expected to cost the world $6 trillion by 2021 - **CSO by IDG***

2. Start to think differently about security because the bad guys already know what you're doing. Start with critical security from the inside out.

   *The median number of days that attackers stay dormant within a network before detection is over 200 - **Microsoft Advanced Threat Analytics | Microsoft***

3. Restore your Trusted LAN. Understand and control who and what connects to you network across physical, virtual, mobile and IoT assets. What you don't know is often where you are most vulnerable.

   *66% of IT Security Professionals Aren't Sure How Many Devices Are Even in Their Environment - **Evil Things Report | Pwnie Express***

4. Incorporate threat intelligence and crowd-sourced feedback into your security framework

   *33% of organizations don't have a threat intelligence program - **Recorded Future***

5. Run frequent, comprehensive vulnerability assessments against your network assets

   *99% of computer users are vulnerable to exploit kits (software vulnerabilities). - **Heimdal Security***

6. Commit to train and re-train your staff to spot malicious traffic. Once is not enough.

   *Human error or system failure account for 52% of data security breaches - **Security Intelligence***

7. Get control of VM sprawl, securely embrace BYOD & mobility and prepare for looming IoT. Network integrity is not possible without a comprehensive understanding and control of all assets connecting to you network.

   *80% of corporate BYOD schemes are "inadequately managed by IT departments." - **Ovum***

About NETSHIELD

NETSHIELD's Mission is to be a trusted provider of cost effective, proactive security solutions to enhance organizations cyber-risk mitigation strategies.

securitysolutions@netshieldcorp.com
1-800-991-3871