Think Differently...

General Data Protection Regulation (GDPR) Preparedness

Over the last few years we've seen a myriad of breach headlines, placing the critical need for enhanced security in the spotlight. In fact, Cybersecurity Ventures predicts cybercrime will cost businesses $6 trillion annually by 2021. The EU's General Data Protection Regulation (GDPR) and US/EU Privacy Shield requirements document enforceable and actionable functionality organizations are required to deploy to ensure preventative capabilities and preparedness are in place in response to this breach epidemic.

When the General Data Protection Regulation (GDPR) goes into effect on May 25, 2018, all companies doing business with individuals located in European Union (EU) member nations must comply with the law's far-reaching provisions. GDPR, affects any company that handles the personal data of EU citizens, whether at an expense or for free. Violation of key GDPR provisions could result in fines of up to 4% of a company's global annual turnover of the previous financial year.

GDPR signifies an official acknowledgement of how important consumer privacy is and how seriously it's being infringed upon. GDPR specifies a compliance framework upon which to build a security infrastructure capable of delivering responsible data privacy. Unfortunately, based on a 2016 survey from Dell, 97% of companies have no plan in place to comply with the GDPR.

No single vendor is capable of delivering a holistic solution to ensure GDPR compliance because many factors must be considered. Although all are required to be in place by May, 2018 establishing preparedness and network due diligence is an excellent starting point. As such, NETSHIELD leverages over a decade of experience delivering security solutions that specifically address two key article requirements specified in the enforceable GDPR framework.

NETSHIELD's GDPR Preparedness Solution specifically addresses articles 32 and 37 of the GDPR framework. Articles 32 and 37 define network system integrity and privacy awareness training, respectfully. Unfortunately, the frameworks are painfully short on details. However, it's imperative that companies invest in preparedness and diligence now to ensure GDPR compliance in early 2018.

The NETSHIELD GDPR Preparedness Solution makes it easy for organizations to deploy a solution to analyze risks, ensure ongoing network integrity, and offer a unique training reinforcement solution capable of delivering GDPR compliance.

Article 32 requires that organizations "Ensure System Confidentiality, Integrity, Availability, & Resilience". The key issue at stake today is that very few organizations operate a "Trusted LAN" making it impossible to ensure network confidentiality, integrity, availability, & resilience. IT has been significantly burdened over the last 5 years with multiple technologies that delivered network efficiencies and economies of scale often at the cost of security and network control.

- Virtualization made it possible to spin up a VM nearly instantly. The problem is that VM sprawl often ensured meaning some of these VMs continue to exist and have remained unpatched and unmanaged for multiple months.

- BYOD and the explosion of corporate mobility has made it nearly impossible for IT to keep up with the security requirements and control of these devices. Mobile security is most often an after-thought largely controlled with the minimal security framework delivered by Wi-Fi credentialing or MDM solutions designed for manageability and not security.

- We are now poised on the cusp of IoT. Cisco predicts that 50-200 billion new devices will join networks over the next 3-5 years. These devices aren't capable of receiving an agent-based security overlay and as such present a significant security challenge for today's security solutions infrastructure.

These and other network control challenges highlight an important question many organizations must face: can you ensure system "Integrity" without total awareness of all assets connecting to networks? NETSHIELD provides this visibility by delivering the ability to discover and control all connecting assets as well as the ability to dynamically block unknown/untrusted assets.

The NETSHIELD GDPR Network Assuredness Solution makes it easy for organizations to deploy a solution to analyze network risks, gain immediate control of corporate LANs and ensure ongoing network integrity.

Article 37 requires that organizations deliver "Awareness raising and training of staff involved in processing operations". In general, this accommodation is delivered as part of corporate security training that is often woefully short of successfully preparing staff to identify and limit the success of diligent advanced, persistent malware.

NETSHIELD offers a unique training opportunity and continuous reinforcing data points that are extremely beneficial to ensure that ongoing training is highly effective and significantly enhanced.

Malware actors continue to evolve and innovate penetrations by targeting one of organizations most vulnerable entry points: the employees themselves. Unfortunately, falling victim to some of these advanced and well disguised attacks happens all too often. The Verizon Data Breach Investigation Report indicates that 30% of phishing messages were opened – up from 23% in their 2015 report. 13% of those opened subsequently clicked the malicious attachment or nefarious link.

The NETSHIELD GDPR Training Awareness Solution framework includes:

- Dynamically block malware, phishing & ransomware from impacting corporate endpoints. IT is instantly notified of these block malware connection attempts.

- Simultaneous notifications to HR can be sent to significantly enhance malware training success by delivering live samples. There is no better substitute for ensuring employees are equipped to spot malware that cyber-criminals continue to evolve.

- Live sampling of malware, ransomware & phishing attacks that illustrates malware sophistication to enhancing employee training.

- Significantly raise employee awareness so they are equipped to effectively join the fight against malware.

Think Differently...

General Data Protection Regulation (GDPR) Preparedness

NETSHIELD is an advanced solution built upon the framework of over a decade of advanced cyber-security solutions. NETSHIELD is well aligned with GDPR requirements as well as industry standards like the UK's Cyber Essentials Assurance Framework and the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, designed to serve companies of all sizes and maturity levels.

GDPR will have a far-reaching impact on other nations outside of the EU. The EU and U.S. are already negotiating the terms of Privacy Shield. This new and more unified approach, however, will require that organizations make adjustments to their current data protection strategy and prioritize placing the appropriate security infrastructure and controls in place.

Below is a compelling matrix defined by SANS Institute illustrating security spending and the calculated effectiveness of the invest-

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

ment. Access Control is defined in the top position and is often an area that is overlooked by many organizations.

The NETSHIELD GDPR Solutions provide organizations with the ability to deploy a program to analyze risks, build a plan for improvement, deliver network integrity and offer training and reinforcement unique to each company's risks and needs, all of which are critical to complying with the GDPR.

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.

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".

Here are 7 key considerations that organizations should consider 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***

Think Differently...

General Data Protection Regulation (GDPR) Preparedness

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