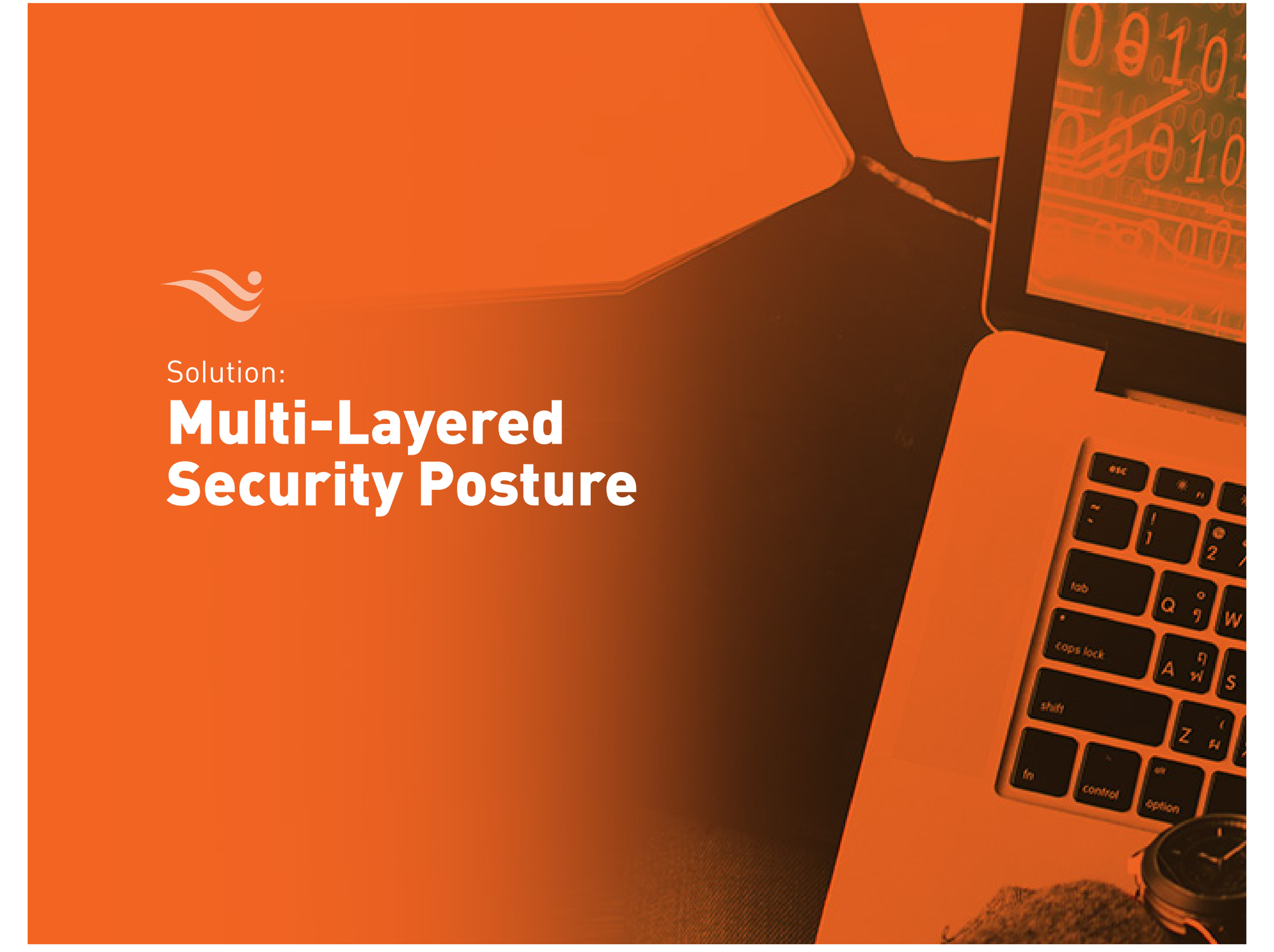
Solution:

Multi-Layered Security Posture



What does your business depend on to operate?

Typically, this consists of data and the systems your employees access for productivity as well as the employees themselves.

Whether it's standard files, email, intellectual property, databases or the users who leverage and manipulate this data, all of these items warrant an enhanced level of security to safeguard.

In this document, we'll go over the best way to mitigate risk to your business' core IT assets and success. Almost all threats come from the internet - a very broad statement. Whether it be viruses and malware, or a malicious entity attempting to trick and exploit your business, they typically traverse a common path.

Leveraging technologies and services at each "pit stop" along this path has proven to be the best way to minimize risk and stop threats. We call this concept the multi-layered security posture. Let's review the path and technologies that protect each layer.

Email Security & Spam Filtering

Gateway/Firewall Level Security Services

Workstation Antivirus & Antimalware

Security Assessment & Policy Development

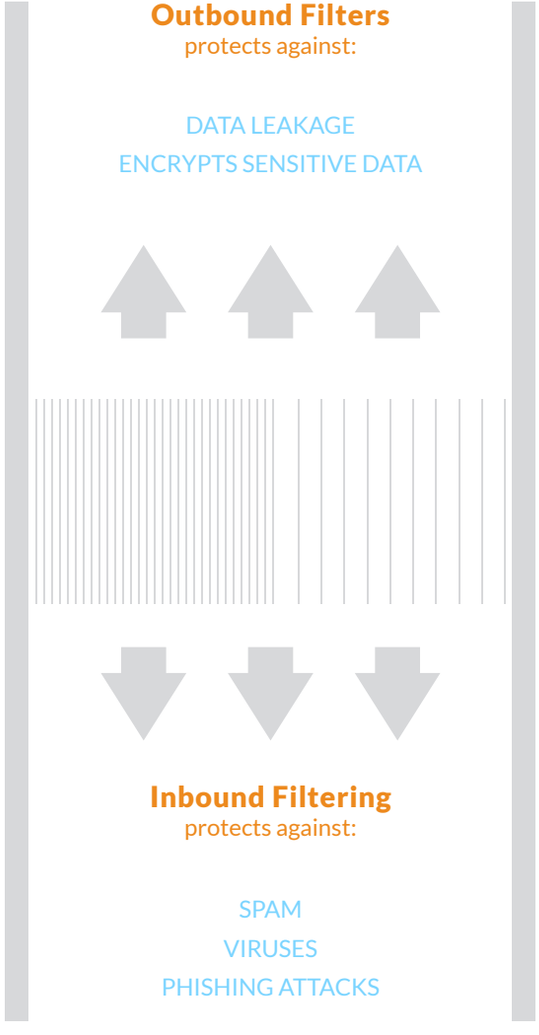
End User Training

Email Security & SPAM Filtering

Email security services are the front lines of email defense. These services act as a filter before email reaches your email system and are applicable for all email systems, including Office 365 and Microsoft Exchange.

Services like Barracuda Essentials provide end-to-end protection of your business email.

Advanced Threat Protection blocks advanced zero-hour attacks. Cloud archiving ensures compliance with retention policies and cloud backup protects you from accidental or malicious data deletion.



Gateway/Firewall Level Security Services

Consider your Gateway as the point where the internet meets your business.

All firewall vendors offer security subscriptions; understanding and implementing them is key.

Gateway security services provide you with a single, integrated bundle of security technologies designed to stop known threats.

Secure your network at the gateway against:

- Intrusion Viruses
- Keyloggers
- Malicious Mobile Code
- Spyware
- Worms
- Trojans
- Adware

& other dangerous mobile apps

Content filtering is also a great way to prevent users from visiting potentially malicious websites.

Workstation Antivirus and Antimalware

Implementing both Antivirus and Antimalware has become a best practice.

Antivirus resides on your computer, actively monitoring and blocking threats. AV products use frequently-updated virus definitions to identify and remove known malicious programs and code.

Other features of AV include identity theft protection, webcam protection and scheduled system scans.

Antimalware is very similar to AV as active and scheduled system scans are also part of its function. What sets AM apart is its ability to inspect and protect attack vectors not covered by traditional AV. Part of MalwareBytes Antimalware suite is the Antiexploit component. This product can stop threats from infecting your system via commonly exploited applications like Microsoft Office and web browsers.

AV/AM proactively block threats. Additionally, they discover and remove threats during scheduled system scans.

These two systems are intended to work side by side, yet independently, compensating each other when one may have overlooked a threat.

Security Assessment & Policy Development

While most businesses have commonalities with IT, every business is unique.

Security assessments help identify areas in need of improvement.

Effective policy development requires a full understanding of how your business operates while customizing industry-wide best practices.

Undergoing a security assessment is the best way confirm proper configurations and/or identify areas in need of improvement.

A common theme in IT is to continuously move forward with technologies. More often than not, this leads to overlooking fundamental or legacy components of your security posture.

A true security assessment looks at every step of your technological staircase, uncovering seemingly basic faults which, without this initiative, may never have been discovered.

Policy development can help address this question as well. Once your entire environment is reviewed, policies can be developed to ensure routine maintenance and auditing occurs across all systems, including your firewall.

End user training

Ongoing end user training is a fundamental component in every company's security posture.

End user awareness is the first and last line of defense. It is possible for non-traditional attacks to circumvent the services listed above.

Common tactics include preying on the human element to trick and deceive.

In some cases, this includes having users infect themselves and/or give away secure information, including credentials.

End user attack vectors are countless; this can include telephone, social media or even an expensive thumb drive "found" in the parking lot.

Having users be on the lookout for suspicious activities and abnormalities can greatly impact threat prevention, response and remediation time.

Having a basic understanding of best practices and being able to raise a red flag when something abnormal is discovered should be welcomed.

Part of policy development and end user training can also include adherence and implementation of secured and well thought-out file and folder structures and associated user permissions.

Compartmentalizing access to certain folders across an organization can help minimize any one particular user's ability to impact the entire business, whether it's unknowingly or malicious and intentional.

the Walker Group
high tech, human touch

www.thewalkergroup.com

20 Waterside Drive
Farmington, CT
06032

860. 678.3530