WHITE PAPER

The Best of Both Worlds

Blending Best Practices with New Security Protocols

Trustwave®

Overview

Cybersecurity is an ever-evolving discipline. Attacks change, technologies come and go, processes adjust, new compliance mandates are regulated, and people are there to hold it all together. But none of this is new, and not likely to change much. It's the way of life for today's security organizations.

While it is important to evaluate and adopt new security programs, it is equally important to leverage tried and tested security best practices that have proven themselves effective at securing your infrastructure. Don't lose sight of existing strategies at the expense of the latest attempts to fortify your infrastructure and keep cyber-attacks at bay.

Security best practices are increasingly being incorporated into regulatory frameworks to establish a minimum standard for organizations. Regulatory agencies step in to establish mandatory requirements when they believe that organizations fail to undertake effective measures to safeguard sensitive data. These regulations grow and evolve over time as the threat landscape evolves. Some noteworthy industry and regulatory requirements include:

- **PCI DSS:** One of the earliest compliance mandates, the payment card industry established information security standards for organizations that process credit cards with the objective of reducing credit card fraud.
- **General Data Protection Regulation (GDPR):** The General Data Protection Regulation (GDPR) was adopted by the European Union (EU) in 2016 to define how personal data should be collected, processed and stored. GDPR went into effect in May 25, 2018. With the comprehensive GDPR guidelines and potentially hefty fines for non-compliance, organizations are scrambling to understand and address its requirements. GDPR affects organizations in any country that are processing or controlling data privacy information in Europe, thus affecting organizations outside the EU as well.

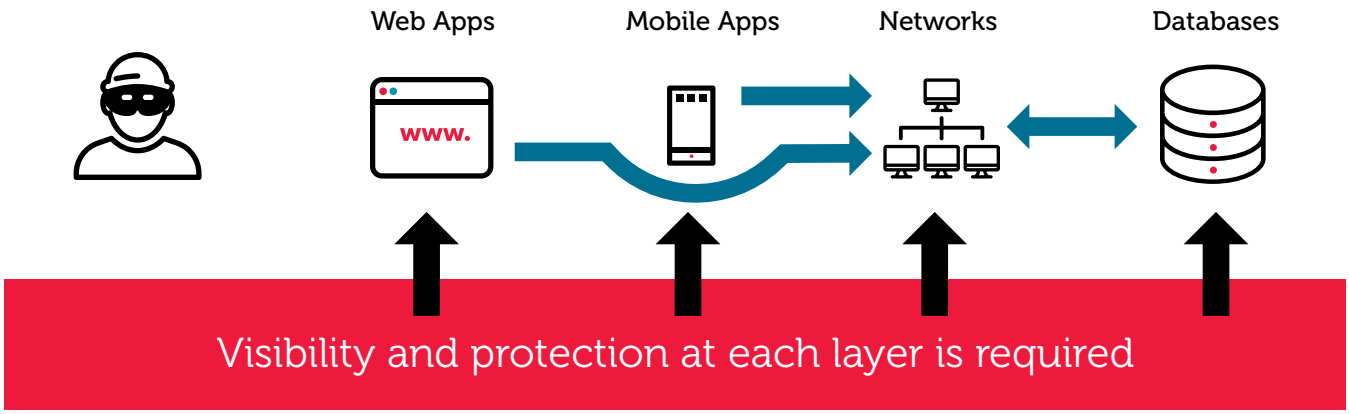
Security professionals have been using some of the same techniques for quite some time. Why? Because they work. Look at these as a gold standard and make them an integral component of your arsenal against cyber threats. We discuss some of these techniques in the next section.

A Holistic, Risk-Based Approach

Securing your network perimeter is no longer enough. Ubiquitous internet access, cloud computing, mobile applications and the Internet of Things (IoT) have expanded the boundaries of your infrastructure far beyond your physical network. And yet, many organizations still take a siloed approach to database, network and application security with the groups responsible for securing them rarely talking together about security. Criminals see data (generally stored in databases) as the prize with networks and applications as the path; they view the whole picture. Organizations must take a similar approach to securing their databases, networks and applications or they risk leaving themselves open to attack due to a limited view of vulnerabilities and risk.

A holistic approach empowers you to manage risk across your entire IT infrastructure - databases, networks and applications - so you can:

- Gain visibility into what you have and what needs to be protected.
- Quickly identify vulnerabilities and analyze the impact of those vulnerabilities.
- Prioritize risk remediation based on risk levels to make the best use of resources.



Security Scanning and Testing

Vulnerability scanning helps you identify assets on your network as well as vulnerabilities and misconfigurations that could potentially give a hacker access. Penetration testing, on the other hand simulates a real world cyber-attack. Penetration testers use tools as part of their work, but they apply threat intelligence and their ingenuity to exploit vulnerabilities, expose assets and illustrate the severity of risk.

Identifying vulnerabilities and conducting penetration testing across databases, networks, and applications are integral components of critical security best practices. Security scanning and testing needs to be conducted regularly, not ad hoc as is all too common. Many organizations also fail to realize how critical it is to rescan and retest after implementing remediation efforts to ensure that vulnerabilities have been successfully remediated.

- Security scanning and penetration testing help you in these areas:
- Identify what needs to be protected with an inventory of assets, data and services on your network.
- Determine which assets are vulnerable and how. Are those vulnerabilities exploitable? If so, what are the consequences?
- Understand the severity of risk associated with each vulnerability. Can you accept the risk introduced by these vulnerabilities? How do you spend time and resources most effectively to mitigate and remediate risk?
- Focus security efforts on the areas that present the highest risk by determining the right level of protection after grouping and prioritizing assets.
- Achieve a security baseline by leveraging the testing and remediation cycle to secure assets as appropriate for the corresponding level of risk.
- Maintain security with regular testing for patch management.
- Incorporating security testing for changes made to your environment that affect risk.

User Roles, Rights and Privileges

Scanning must include the understanding of user roles, rights and privileges in addition to identifying vulnerabilities and misconfigurations. This includes identifying excessively privileged user accounts. The only way to establish meaningful controls that track how users interact with the data, or to capture an audit trail for use in a breach investigation, is to know who has access to what data and why/how they have been granted that access. One particularly challenging question that many organizations still face is: "Who has access to my sensitive data?".

Another important security feature is the principle of least privilege (POLP); provide users with only the bare minimum permissions required to perform their jobs. Once established, a regular review of user permissions should be conducted to confirm no unnecessary privilege escalations have been granted.

Threat Intelligence – Teaching an Old Dog, New Tricks

Modern security scanning and penetration testing solutions utilize global threat intelligence to enhance the traditional techniques. Robust scanning and testing solutions must be supported by vast insight into the latest vulnerabilities, attack vectors, exploits, malware and security breaches gathered from extensive security research, penetration testing and incident response engagements. Scanning and testing tools and techniques can only go so far without this highly detailed threat intelligence.

Security Maturity and Risk Tolerance

Organizations must understand their level of risk tolerance – how bad will it get when they do get breached and what are the consequences and costs - and what level of maturity is required to minimize the impact of a breach.

Risk tolerance and security maturity are different for every organization. Risk tolerance is a business level decision that requires cross-functional analysis and agreement. Security scanning and testing is one (important) step towards determining the current risk level.

Security maturity is book ended by current and future state. Based on the agreed upon risk tolerance level, organizations determine what future state means to them. From there, a plan is developed, and people, process and technology are utilized to build against the plan and, finally, run against the plan to achieve the targeted future state. This plan/build/run methodology successfully allows the security team to transform the way they protect the company and meet business risk tolerance objectives. This is the Security Maturity journey.

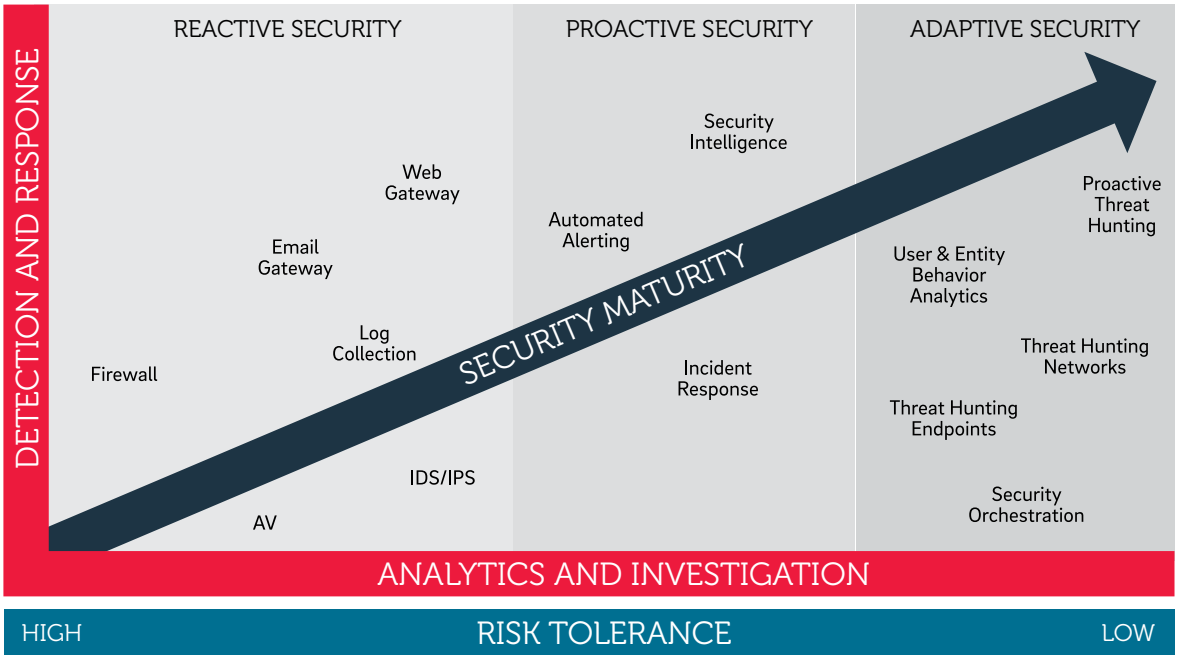


Figure: Assessing an Organization's Security Maturity and Risk Tolerance Level

How to Overcome a Daunting Prospect

With attacks growing exponentially in volume and complexity, organizations face an almost insurmountable challenge to implement effective security programs at a time when security resources are severely limited. They struggle with inadequate time, funds, skillsets and headcount. So how to overcome this huge obstacle? This is where businesses can benefit by partnering with a Managed Security Service Provider (MSSP) who can provide the security expertise, skill sets, threat intelligence and technologies to protect against the barrage of cyber-attacks. Partnering with an MSSP gives you access to the much-needed security expertise and resources, allowing you to offload security tasks, stretch your security budget and improve security outcomes.

Offloading tedious or bulk security tasks

- **Staff Augmentation:** Organizations facing IT security hiring shortfalls or excessive turnover should consider MSSPs for staff augmentation. Organizations should first apply MSSPs to where they will obtain the largest improvement in security posture or the biggest impact on freeing up internal staff for more strategic tasks.
- **Flexibility:** The degree of offloading to the MSSP is flexible ranging from tasks that can be partly delegated to the MSSP, or more fully managed (such as bulk event monitoring or threat correlation) by the MSSP, freeing up in-house staff to focus on escalated alerts or more strategic projects as needed.
- **Improved security coverage:** MSSPs help deliver broader security coverage, address compliance requirements and see more clearly how to allocate resources to ensure one has met their organization's security needs for now and the future. This in turn reduces risk of the types of avoidable incidents that threaten IT security team members' jobs.

Stretching Security Budgets

MSSPs can help you extend your security budget and give you access to security expertise and operations without having to invest in them:

- **Access to global, 24x7 Security Operations Centers (SOCs):** This is crucial to rapid detection and response to security events and breaches. An around-the-clock SOC means there are experts available whenever a security event occurs.
- **Security operation benefits for IT departments:** IT Departments get access to world-class SOCs that meets high-facility standards at a fraction of the cost of building their own centers. They get access to seasoned security experts, support from a platform of global threat intelligence, obtain mature best practice procedures - all of which improve responsiveness and efficiency to help prevent or contain breaches sooner.
- **Increased efficiencies:** MSSPs develop high-level acumen by being exposed to a large number of organizations, and each individual MSSP client gains the benefit of the MSSP's streamlined skills. MSSPs also stay up to date on security best practices.

Improving Security Outcomes

Using an MSSP to fill critical roles and stretch budgets can have direct and indirect effects on improving security outcomes. These include:

- **MSSPs help cover more threat vectors.** A MSSP does this by augmenting one's team, bringing more expertise to bear, using their time and tools more efficiently, adjusting to new threats faster and freeing up internal resources to add higher-order value.
- **MSSPs use up-to-date and most effective security practices.** MSSPs are pioneers of and leading-edge implementers of new security best practices. MSSPs have greater specialization and economies of scale from providing similar services to many organizations. They have the advantage to adjust and refine security techniques iteratively for greater effectiveness.
- **MSSPs are quick to spot new and emerging threats.** Having access to a large team of security specialists working closely together, monitoring a large portion of the internet and keeping each other abreast of fast-moving developments at various enterprises gives MSSPs the advantage of learning about and mitigating emerging threats much quicker than in-house experts.

Trustwave®

TRUSTWAVE.COM