FROST & SULLIVAN

A Frost & Sullivan eBroadcast Executive Summary

LEVERAGING VULNERABILITY MANAGEMENT FOR ENHANCED SECURITY

Analysis and key take-aways to help you:

- Ensure the most accurate vulnerability scan data
- Alleviate security data overload and leverage state-of-the-art security technology
- Bridge the gap between IT and Security Operations

View this eBroadcast at:
www.frost.com/scanengine

MODERATOR

- **Chris Kissel**
  Senior Industry Analyst, Network Security
  Frost & Sullivan

PANELISTS

- **Dr. Edward G. Amoroso**
  Founder and Chief Executive Officer
  TAG Cyber LLC
- **Gordon MacKay**
  Executive Vice President Chief Technology Officer
  Digital Defense, Inc.

OVERVIEW: THE STATE OF VULNERABILITY MANAGEMENT TODAY

Over the last several years, the number and magnitude of cyber security breaches has steadily increased. To date, numerous institutions, big and small, both private and public, have disclosed that databases containing customer identities and other private information have been exposed and compromised. As Chris Kissel, eBroadcast Moderator and *Senior Industry Analyst, Network Security,* Frost & Sullivan stated, "The feeling that attackers can disrupt businesses or infiltrate files can leave people numb."

Among the most high profile cases were the recent Yahoo data breach that left over one billion identities exposed and the U.S. Office of Personnel Management, where as many as 22 million identities may have been compromised. Hacked information included health and financial records. At the Fortune 500 organization Dun and Bradstreet, approximately 33.6 million files were subject to exposure. In addition to being disturbing, such breaches can have long term repercussions, adversely affecting individuals and disrupting businesses for years after the breaches have occurred.

Yet, there is hope for organizations and their employees alike, in the form of sophisticated cyber defense tools and security safeguards and solutions. There are numerous strategies and tools currently available that can create friction for hackers and at least dis-incentivize those who would attempt to breach security.

In fact, according to the Alliance Cyber Insurance Group, up to 80% of all cyber-attacks can be prevented with basic database management. This statistic was also corroborated by Verizon in a recent data breach report.

ESTABLISHING FOUNDATIONAL SECURITY MEASURES

As the chart below more fully illustrates, there are several foundational security measures that can be taken to guard against breaches. They include writing strong and secure code, creating strong identity authentication and access management features and adhering to industry best practices that include multi-level security for networks, servers and cloud and mobile devices.

Yet, overall, it used to be easier to provide security and protect networks. Throughout the 1990s, network servers could be protected by firewalls and other security measures.

Additionally, most security strategies before 2008 involved scanning servers and on-premise desktops with only a few endpoints, or endpoint devices including desktop or laptop computers. Before the cloud, mobile devices and remote Wi-Fi access, firewalls were often sufficient to safeguard networks and data.

"There is hope for organizations and their employees, in the form of sophisticated cyber defense tools and security safeguards… that can create friction for hackers and at least dis-incentivize those who would attempt to breach security."

— Chris Kissel
Senior Industry Analyst, Network Security
Frost & Sullivan

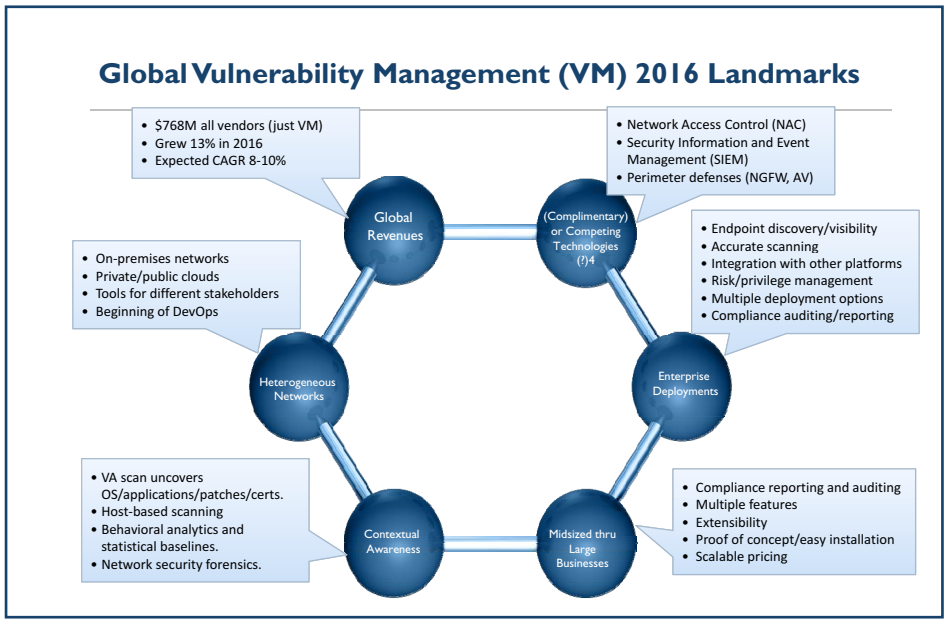
VULNERABILITY MANAGEMENT (VM)

Today, the security game is more complex and requires more sophisticated processes and approaches. Now, leading the chain of strong IT safeguard and security essentials is what is known in the industry as Vulnerability Management (VM). Vulnerability Management is the formal reporting of what is found after a vulnerability assessment scan, a script of known vulnerabilities against a known endpoint. The VM vendor can shape the report to prioritize vulnerabilities, or to meet internal or external compliance standards. The following information obtained is very important:

- Detection of vulnerable endpoints (or detection of endpoints, period)
- Proof of compliance with industry guidelines and standards

"Vulnerability Management assessments allow you to assess risk at a network level. Then you need to prioritize the risks and assign them to teams too. Humans play a really big role in security breaches…"

— Gordon MacKay
Executive Vice President and Chief Technology Officer
Digital Defense, Inc.



Gordon MacKay, *Executive Vice President and Chief Technology Officer,* Digital Defense, Inc. stated, "VM assessments allow you to assess risk at a network level. It is an ongoing process of scans and assessments. Then you need to prioritize the risks and assign them to teams too. Humans play a really big role in security breaches, so any assessment should include a human assessment too."

As Dr. Edward G. Amoroso, *Chief Executive Officer,* TAG Cyber LLC, summed it up later in the discussion: "When it comes to vulnerability management assessment, the word holistic comes to mind. Virtual management scanning can lead to an understanding of posture, where to invest and where there are soft spots. It is a holistic umbrella showing where to direct actions and investment."

Done correctly, vulnerability scans and vulnerability management enable triage when an event is investigated, and ideally, generate a golden state where networks and endpoints are properly fortified. Importantly, as Chris Kissel observed, "VM has grown to scale with the heterogeneous networks of 2017. It is also important to remember that VM is an ongoing process."

FROST & SULLIVAN ASSESSMENT OF THE VULNERABILITY MANAGEMENT MARKET

Frost & Sullivan believes that the majority of devices scanned are still on premise personal computers. However, with the installation of local agents and other 3rd party connectors, VM can cover many remote computing scenarios. Compared to other current security management providers, VM solution providers are in good shape. The data they glean is very rich. And, although VM competes with other technologies providing contextual analysis of end points, Frost & Sullivan expects the global VM market to grow 8-10% over the next five years.

"According to the Alliance Cyber Insurance Group, up to 80% of all cyber-attacks can be prevented with basic database management."

— Chris Kissel
Senior Industry Analyst, Network Security
Frost & Sullivan

"Virtual management scanning can lead to an understanding of posture, where to focus and where there are soft spots. It is a holistic umbrella showing where to direct actions and investment."

— Dr. Edward G. Amoroso
Chief Executive Officer
TAG Cyber LLC

Today's IT marketplace includes new and expanding service offerings including compliance reporting and auditing, web applications and continuous monitoring. As often noted, in many quarters, there is still some cynicism about cloud based security.

Toward the evolution of VM, here are a few other notable statistics:

- In the years 2016–2021, the SaaS form-factor will become the largest product group in terms of revenue. In 2021, SaaS VM is projected to have revenues of $537.5 million
- North America is the region that accounts for most VM sales accounting for 76.8% of all global VM revenues in 2016. In 2021, Frost & Sullivan expects that share to grow to 77.8% of all revenues
- The market leaders in VM either have or are developing complementary technologies that leverage vulnerability management such as continuous monitoring and incident detection and response (IDR)

VULNERABILITY MANAGEMENT CHALLENGES

One of the biggest issues associated with vulnerability management revolves around when to do it. And, then, after you have done the assessments and VM work, what do you do with the recommendations. The experts on this eBroadcast panel agreed that what to do next can be the most difficult aspect of enterprise security. Even with great tools, metrics and data, it can be difficult to know what to do with the findings, and what to choose from among any number of possible IT solutions or strategies.

In addition, there are also many challenges related to the accuracy of data and measurement in mobile environments. Accuracy is very important with VM and the sharing of the data obtained.

One particular challenge involves scan to scan host correlation. To start, there are many different scanning technologies to choose from. Often, organizations will use a technique known as network unauthenticated scanning, where scanning is remote to the devices, then sends out internet messages, based upon device responses. This technique allows for the scanning of devices and open ports and can highlight configuration issues and other vulnerabilities.

Organizations will usually use this technique to perform regular scanning operations, but it is contingent upon the technology being able to correlate a given host at different points in time. The problem is, these variables change more often than one would think, and the data collected is often faulty or incomplete. In fact, Digital Defense recently did a study about how often network locations change, and the findings were alarming as this severely impacts the accuracy of results. Gordon McKay, *Chief Technology Officer* of Digital Defense Incorporated, theorized that many organizations have limited algorithms and therefore "get it wrong." The question then becomes: how do you solve this challenge?

"Digital Defense uses a patented matching algorithm technology that takes into account all factors the scanner detects, including IP address, different host names, operating systems, device type and more."

— Gordon MacKay
Executive Vice President and Chief Technology Officer
Digital Defense, Incorporated

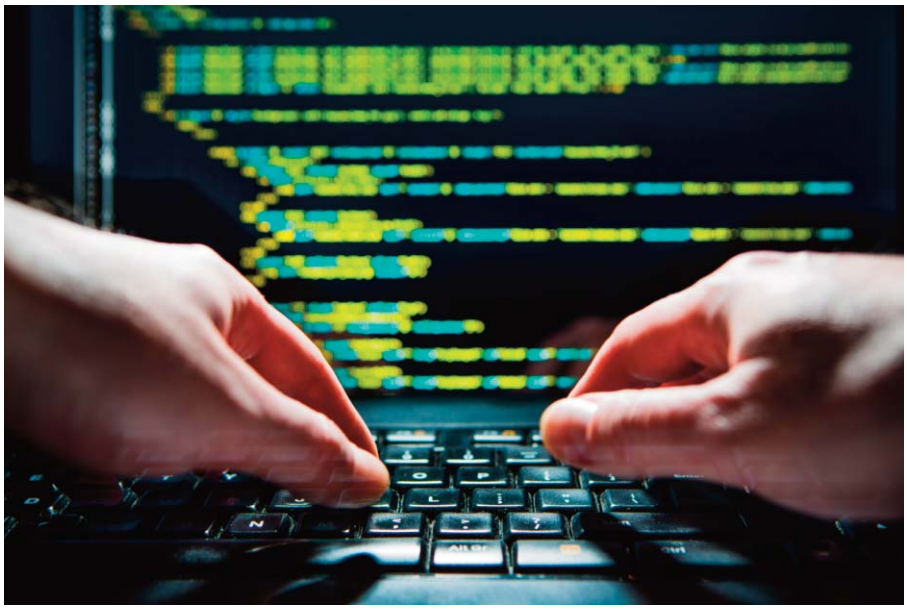
CHOOSING THE BEST TOOL

Many technology solution providers use scanning processes offering limited matching algorithms. This often results in inaccurate data and reporting. As stated, many times, when the vulnerability assessment process is done incorrectly or incompletely, companies end up with inaccurate reports. It might be reported that something is fixed when it really isn't...or report that there is a new vulnerability, when there is not.

Also, as Moderator Kissel observed, VM tools must be easy and intuitive to use and in the case of smaller and mid-sized companies, there has to be a mechanism where VM tools can be integrated into every day IT work flow. It is incumbent upon network tool security providers to address this reality.

To counteract these issues, Digital Defense, a managed security assessment provider, uses a patented matching algorithm technology that takes into account all factors the scanner detects, including IP address, different host names, operating systems, device type and more. Correctly assessing all of these variables simultaneously with the advanced algorithm technology effectively amounts to something like a"fingerprint match" – the holy grail of security.

In fact, the Digital Defense approach leads to highly accurate scan-to-scan data across time and cuts down on false positives in organizational ecosystems, creating a cascade of positive effects. This also means organizations spend less time tracking vulnerabilities and unraveling issues.



PREVENTION TECHNOLOGY VERSUS RESPONDING TO DATA ATTACKS

Pertinent to any current discussion of security management is the issue of proactive versus reactive security. Proactive approaches include measures taken with the goal of preventing host-based or network-based attacks from compromising systems. Reactive security includes the procedures that organizations use once they discover that systems have been compromised by an intruder or attack program, akin to a Disaster Recovery Program. It must be noted that VM is a proactive solution, but some combination of proactive and reactive approaches is necessary for all organizations, and requires an appropriate allocation of resources and budget by companies.

Another important security assessment issue involves measurement and metrics of security effectiveness, so often a question the executive team wants answered. As Dr. Edward G. Amoroso, *Chief Executive Officer,* TAG Cyber LLC, speculated, the big picture answer may very well be that it is nearly impossible to measure something as vast and complex as ongoing network security, but, conversely, there are some tangible tools and measurements that may be applied.

For instance, Digital Defense, offers a measurement called Security GPA®. This tool allows them to measure based on one scanned host, or a group of hosts, expressed as a numerical value ranging from 0 to 4.0, the familiar GPA reference point from school days. These measurements can be very granular. Additionally, Digital Defense can compare a specific client's Security GPA score with other organizations in their client base, allowing them to benchmark other companies. Digital Defense can also measure Security GPA by industry.

As noted above, the age we live in is rife with security issues and data breaches. To keep their infrastructures secure, organizations need multi-level defense tools and processes, including vulnerability management. For smaller organizations, excellent tools like vulnerability management can do most of the job. Larger enterprises require more complex solutions, but all organizations can benefit from best-in-class solutions and providers who are experienced in the field and leverage the latest technologies and most up to date research.

FINAL THOUGHTS

In the Frost & Sullivan study, *Vulnerability Management (VM)–Global Market Analysis, Adding Actionable Intelligence to Network Scan Technology,* Digital Defense Incorporated was cited as having the Best VM Scan Engine. The fundamental strength of its VM solution is that it accurately tracks the host controls in a network (ephemerally and over time), and, as such, as the host environment is understood, and the chance for false positives from scan data from endpoints is greatly diminished.

But even as Digital Defense has a strong VM platform, the company must continue to innovate as VM vendors are building additional services onto their platforms including incident detection and response (IDR), asset discovery, and continuous monitoring. Additionally, Digital Defense also competes with vendors from SIEM, NAC, next generation firewalls, and other network perimeter defense technologies are creating scan technologies that also provide contextual information about the endpoint.

ABOUT DIGITAL DEFENSE, INCORPORATED

Founded in 1999, Digital Defense Inc. is a premier provider of managed security risk assessment solutions, protecting billions in assets for small businesses to Fortune companies in over 65 countries. Our dedicated team of experts helps organizations establish an effective culture of security and embrace the best practices of information security. Through regular assessments, awareness education and rapid reaction to potential threats, our clients become better prepared to reduce risk and keep their information, intellectual property, and reputations secure. Learn more at www.DigitalDefense.com

ABOUT TAG CYBER

The vast majority of enterprise cyber security teams can not afford the proper guidance and analysis required to protect their infrastructure from advanced cyber attacks. TAG CYBER decided it was time to *democratize expert cyber security analysis*. We do this through a steady stream of original content, centered on our flagship *TAG Cyber Security Annual*, a three-volume publication that is a freely available download. TAG CYBER also offers a daily variety of cyber security content through our website, social media, and related distribution channels. We complement this with customized training courses, expert cyber security consulting eBook publications, and related services such as professional CISO coaching. Learn more at www.tag-cyber.com

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation, and implementation of powerful growth strategies. Frost & Sullivan leverages 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from more than 40 offices on six continents. Learn more at www.frost.com

DISCLAIMER

This Executive Summary discusses key insights and excerpts from a live presentation and discussion by Frost & Sullivan, TAG Cyber LLC and Digital Defense, Incorporated on April 13, 2017. This summary presents industry insights, best practices, and case studies discussed by the presenters, in the context of the live presentation and discussion. For more details, visit www.frost.com/scanengine. Frost & Sullivan is not responsible for the loss of original context or the accuracy of the information presented by the participating companies.