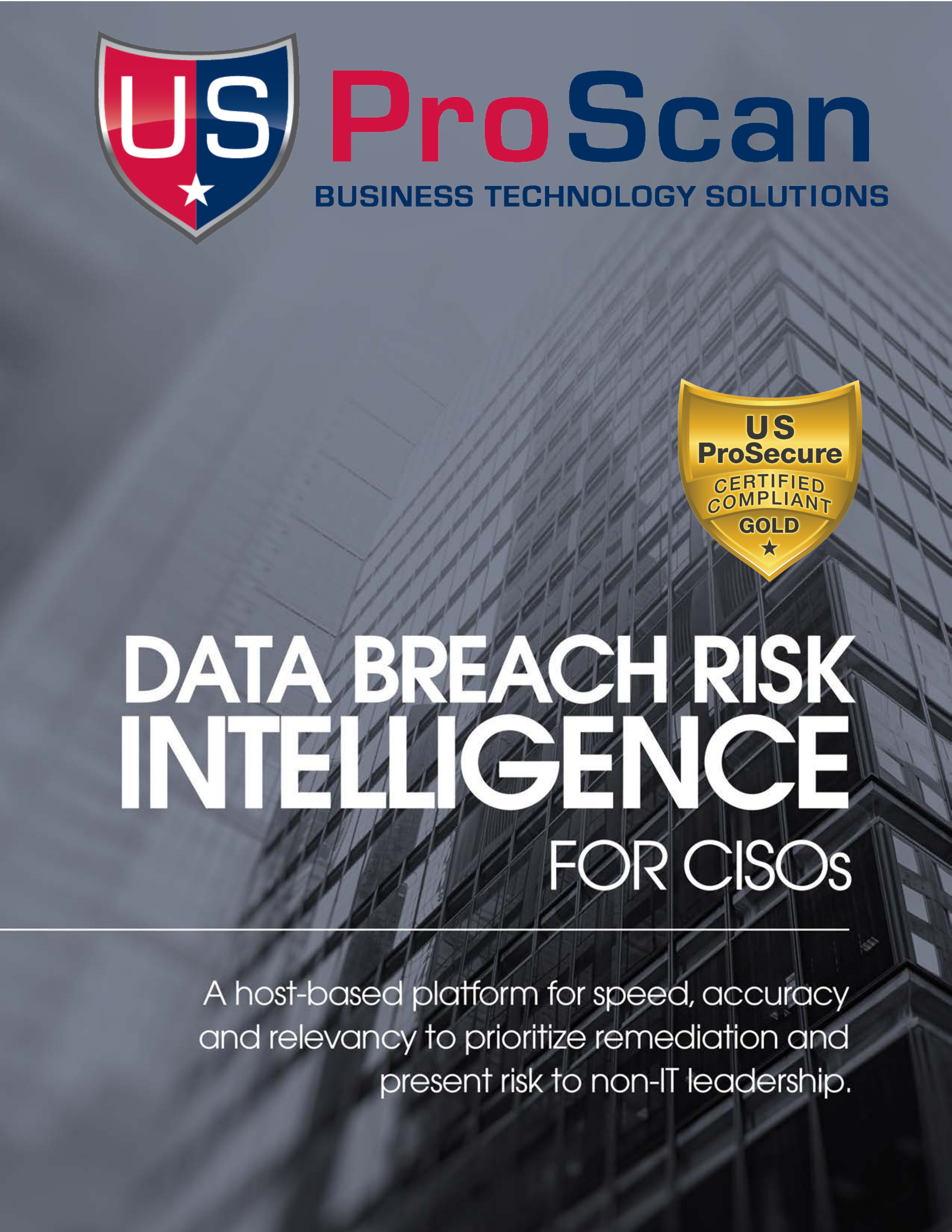
US ProScan

BUSINESS TECHNOLOGY SOLUTIONS



US ProSecure CERTIFIED COMPLIANT GOLD ★

DATA BREACH RISK INTELLIGENCE FOR CISOs

A host-based platform for speed, accuracy and relevancy to prioritize remediation and present risk to non-IT leadership.

Contents

INTRODUCTION

Data breaches are a top priority for organizations

With over 135 million records stolen in just the first half of 2015, understanding the likelihood of a data breach has become a top priority for organizations.

So much so, in fact, that industry analyst Gartner stated in a recent report, "Breaches demand active engagement from the business units and the Board".

Legacy solutions are not relevant outside of IT

According to the 2014 IBM Chief Information Officer (CISO) Security Assessment, 82% of security leaders participate in strategic/C-suite meetings quarterly or more frequently.

However, legacy solutions are not designed for non-IT leaders, such as C-level executives, business unit leaders and the Board. There is no accurate way to quantify risk in financial terms, and data is not tied to business outcomes. The results: mis-matched priorities between business leaders and the security team, difficulty in implementing company-wide security initiatives, and a fight to justify the security budget.

This white paper outlines:

- The technology reasons why existing solutions are not relevant outside the IT department
- How a new host-based platform revolutionizes the speed, accuracy and relevance of data breach risk detection
- The benefits to the organization

THE PROBLEM

Existing technologies are not designed for CISO-level intelligence needs

There are three major weaknesses in current technologies that are barriers to communication between CISOs and business leaders:

1. **Multiple legacy platforms**

Existing technologies were built for yesterday's IT needs. In these solutions, data and vulnerability detection are on different platforms, requiring multiple tools for the discovery process. Data discovery is slow and complex. Vulnerability management is also slowed by networks and credentials.

2. **Analytics not designed for people outside the IT department**

Legacy solutions were designed to present data to technical security professionals. They do not provide a complete view of the total risk posture of the organization, how that posture has changed over time and – most importantly - what that means to the bottom line.

3. **Analytics not automated, not real-time**

Security teams have many demands placed upon them and remediating every device on a network is rarely an option. In addition, analysts must spend days or weeks translating data to be relevant to non-IT leaders.

An intelligence platform for speed, accuracy and relevance

US ProTech has developed the industry's first data breach risk intelligence platform that automatically puts a real-time dollar value on an organization's security risk.

The patented host-based technology provides a clear view of total risk posture relevant to CISOs and non-IT business leaders through:

A single platform

US ProTech combines data discovery, vulnerability management and access permissions into a single report. With it, a significantly clearer and more accurate risk picture appears for each device, team and organization.

C-level ready analytics

CISOs need analytics that can be understood by non-IT leaders and mapped to business priorities. US ProTech answers:

- What data is unprotected and who has access to it?
- How can it be compromised?
- What will it cost me when breached?

With the above intelligence, CISOs can justify resources to CFOs and engage business leaders on priorities.

Real-time automation

Because US ProScan calculates the dollar value of risk automatically for each device on the network, CISOs can focus their resources on remediating devices with the largest financial risks. Analysts can spend their time on strategic execution instead of crunching data for C-level presentations.

> CISOs need analytics that can be understood by non-IT leaders and mapped to business priorities.

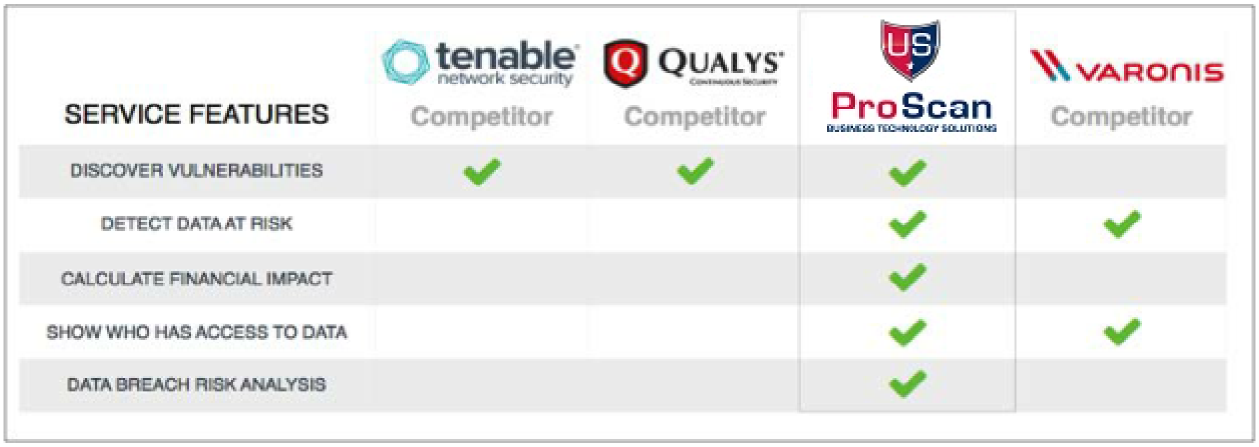
TECHNOLOGY

PERFORMANCE

Combining data and vulnerability detection

Most existing products were either designed to detect data at risk or vulnerabilities, but not both (Figure 1). This means increased intrusiveness and an incomplete view of an organizations risk exposure.

Figure 1: *Legacy solutions cover only data or only vulnerabilities, making them more intrusive and unable to provide a comprehensive breach risk overview.*



SERVICE FEATURES	tenable network security Competitor	QUALYS Competitor	US ProScan BUSINESS TECHNOLOGY SOLUTIONS	VARONIS Competitor
DISCOVER VULNERABILITIES	✓	✓	✓	
DETECT DATA AT RISK			✓	✓
CALCULATE FINANCIAL IMPACT			✓	
SHOW WHO HAS ACCESS TO DATA			✓	✓
DATA BREACH RISK ANALYSIS			✓	

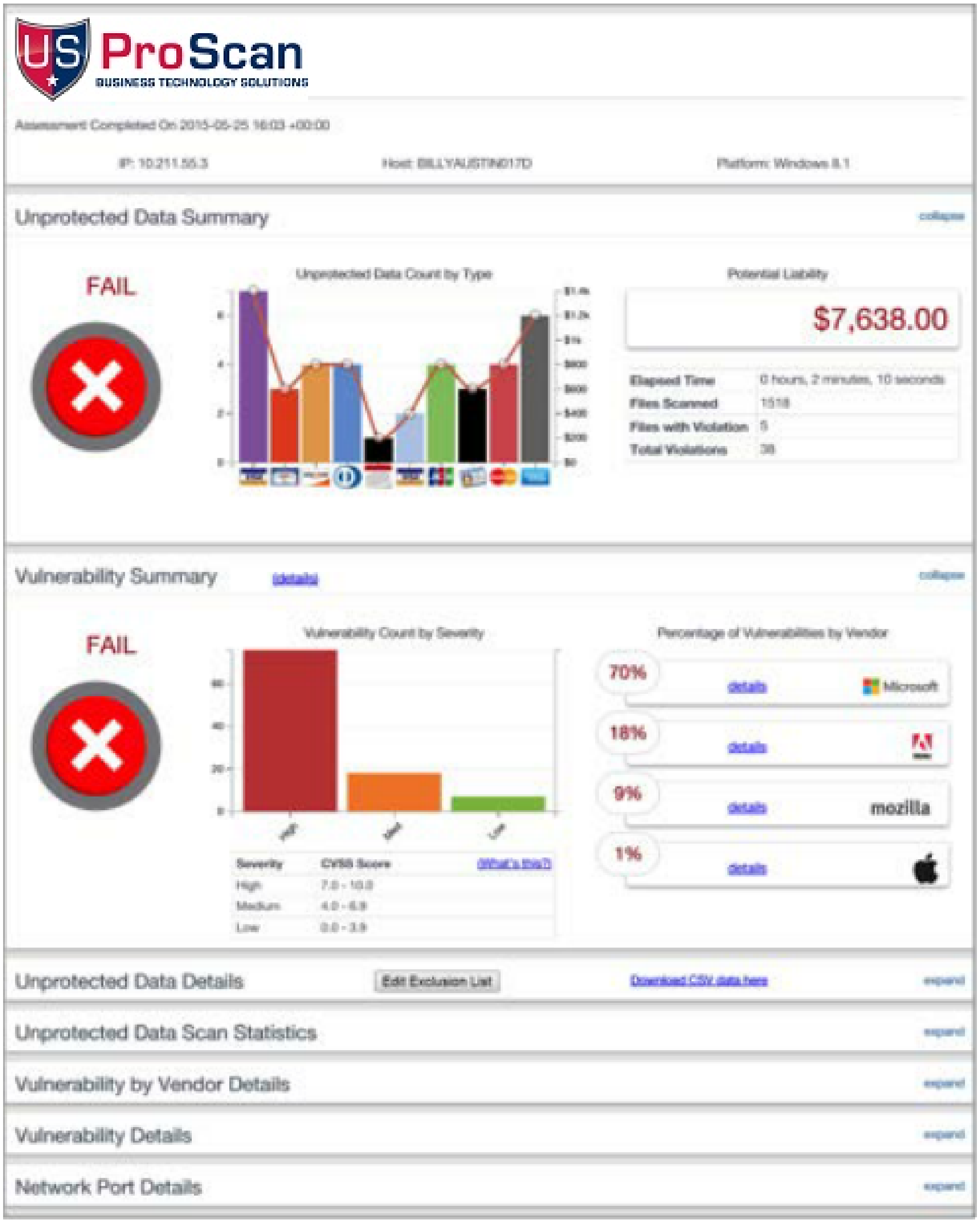
Alternatively, there are many advantages of US ProScan's combined platform for data at risk and vulnerabilities:

A combined data and vulnerability discovery tool benefits device users:

1. It's less intrusive. Scan once for updated information on both data and vulnerabilities.

2. It's more actionable. The device owner can see the Security Number, the financial liability dollar figure, for each of his/her devices. (Figure 2).
3. It's easier to manage for security/IT operation teams. They can view comprehensive total-exposure reports for the entire organization.

Figure 2: *Sample Device Risk Report that includes data at risk, access information, vulnerabilities and the Security Number, the risk liability calculated in dollars.*



US ProScan
BUSINESS TECHNOLOGY SOLUTIONS

Assessment Completed On 2015-05-25 16:03 +00:00

IP: 10.211.55.3 Host: BILLYAUSTIN017D Platform: Windows 8.1

Unprotected Data Summary collapse

FAIL

Potential Liability

$7,638.00

Elapsed Time	0 hours, 2 minutes, 10 seconds
Files Scanned	1518
Files with Violation	5
Total Violations	38

Vulnerability Summary (details) collapse

FAIL

Severity	CVSS Score	(What's this?)
High	7.0 - 10.0	
Medium	4.0 - 6.9	
Low	0.0 - 3.9	

Percentage of Vulnerabilities by Vendor

70%	details	Microsoft
18%	details	
9%	details	mozilla
1%	details	

Unprotected Data Details Edit Exclusion List Download CSV data here expand

Unprotected Data Scan Statistics expand

Vulnerability by Vendor Details expand

Vulnerability Details expand

Network Port Details expand

Unprotected Data Count by Type
0
2
4
6
$0
$200
$400
$600
$800
$1k
$1.2k
$1.4k
Vulnerability Count by Severity
0
20
40
60
High
Med
Low

Overcoming historically slow and complex data discovery

Many organizations have attempted to deploy Data Loss Prevention (DLP) products with limited success because of how complex and resource-intensive the technology is, and how easy it is for pre-set rules to miss crucial risks. Even with dedicated appliances managing the DLP, a solution designed to detect data in motion that is used for data at rest can be prone to months-long deployments or risk missing crucial unprotected data. (Figure 3)

Complexity

Endpoint DLP is a very complex solution that is primarily designed to prevent sensitive data from being sent out of an organization. In order to be effective, endpoint DLP products require persistent agents and must perform extensive hooking of operating system and application APIs to prevent users from copying, pasting and emailing sensitive information. This often leads to the unintended side effect that users are prevented from being productive in their daily tasks.

US ProScan is solely focused on identifying sensitive data at rest on various endpoints. It doesn´t require a persistent agent and doesn´t perform any operating system or application hooking. It compliments existing security technologies and is non-intrusive, eliminating any impact on user productivity.

Performance

Because DLP solutions were built primarily for blocking data in motion, detecting data at rest is a secondary function added by vendors based on customer feedback to determine where sensitive data already exists. Because this functionality was an afterthought, typical performance characteristics are not appropriate for most use cases. Most customers can observe extreme CPU and memory utilization during data discovery scanning by these legacy solutions.

US ProScan has been specifically built with performance in mind. Due to the patented endpoint scanning capabilities, CPU utilization and memory footprint are always designed to be low impact on the device, allowing users to work freely without noticing any degradation in their daily system performance.

Large volumes of data

As organizations grow, so does the amount of data generated and many customers who have evaluated or implemented named competitors in this space have reported difficulty scanning large volumes of data typically found on multi-terabyte storage units.

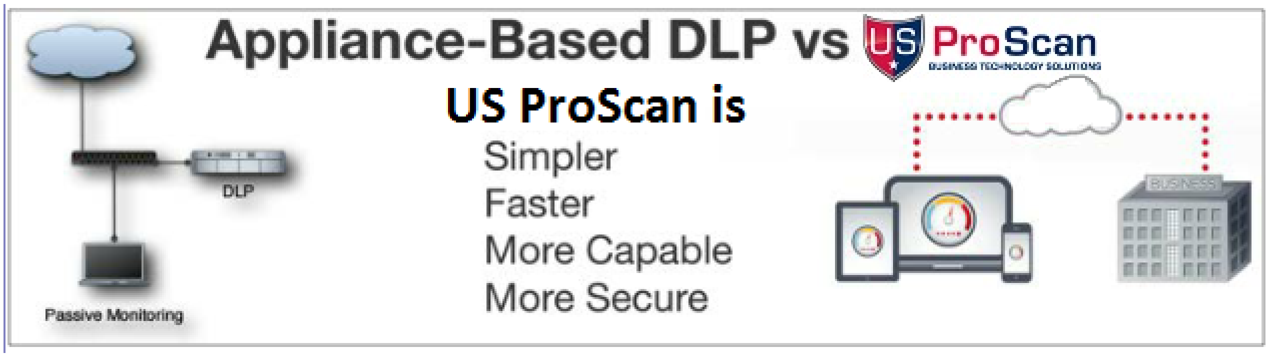
US ProScan is designed to be highly efficient when scanning high capacity storage systems and completes scans more efficiently then any of the competitors in the space. It utilizes a highly optimized data scanning algorithm as well as contextual analysis of the data being scanned in order to reduce overall scan times, reduce memory utilization and increase detection rates.

Security

Many of the DLP and Data Discovery technologies available are marketed to be security solutions, but often fall short when true security measures are evaluated. For instance, most solutions do not redact sensitive information when reporting violations to their management console.

US ProScan delivers security throughout its platform. When sensitive data is discovered, it is redacted before being sent to the management console. This prevents replication and potential unwanted exposure of sensitive data. The US ProScan Data Breach Risk Intelligence platform provides security logging of management events, role based access controls and utilizes encryption from endpoint to cloud to secure data transmissions. All endpoint-scanning components are cryptographically signed and verified prior to execution.

Figure 3: *DLP solutions require long deployments, are slower and prone to missing critical data at risk.*



Appliance-Based DLP vs US ProScan

US ProScan is

Simpler

Faster

More Capable

More Secure

1. *Where is my sensitive data and who has access to it?*
2. *How can hackers and thieves get to my data?*
3. *What will it cost if I´m breached today?*

File auditing with share permissions and file finding

File Auditing solutions typically determine which users and groups have rights to files and folders in the organization. They are typically focused on servers and can sometimes include capabilities to discover sensitive data.

US ProScan provides comprehensive analysis of the permissions assigned to users and groups on the files for which sensitive data is discovered. Unlike most of the file auditing tools, this analysis is also performed on workstations. In addition to the permissions, US ProScan discovers if the file is shared, and reports on the path.

Reporting on share permissions can be extremely helpful in detecting various insider access threats as well as determining over-zealous sharing on laptops and desktops. For example, US ProScan will uncover if a user is sharing his or her home directory with access to everyone.

In addition to permissions reporting, US ProScan can be used to detect the presence of specific files across all desktops, laptops or servers. For example:

- In an incident response scenario, given an MD5 hash of a malware sample, US ProScan can scan all systems and detect the presence of the given malware.
- US ProScan can detect unprotected ACH file information on devices at a bank or credit union.
- US ProScan can find unprotected intellectual property through a custom search for manufacturers, pharmaceutical companies and law firms.

Vulnerability management without network slowdowns or credential limits

Most organizations have deployed a vulnerability management solution, but continue to struggle with ongoing threats because of several crucial limitations in past solutions that slow down detection and limit success. Performance-sucking network scans can slow your business to a crawl or result in devices that never complete a full assessment. Issues with credential management often result in scans that miss key directories or leave security administrators scrambling to manage the credentials individually for every device.

Network-based is an outdated approach

The main competitive vulnerability management tools primarily use network-based scanning technology. But network vulnerability scanning solutions can't obtain information about which assets are affected by critical vulnerabilities in a timely manner because of the basic architecture:

- Each centralized network-scanning appliance must have a conversation with each device to be scanned.
- It must send packets back and forth over the network, authenticate, evaluate and repeat the cycle for each device.
- This can take hours if not days or weeks for very large networks.

Plus, these tools rely upon remote administrative authentication to perform a detailed assessment of the device. If the scanner is run without credentials or non-authenticated scans, the output is comparable to a port scan. This leaves a huge potential for false positives and false negatives.

Because US ProScan is a host-based technology the fundamental limitations of network scanning are no longer a problem. The network won't buckle because it's inundated with scanned packets transmitting back and forth and scans will finish more quickly. Plus, because the scan is host-based, there are no issues with insufficient permissions that keep vital drives and folders from being protected.

Endless credentials cause headaches

The requirement to provide credentialed scans for detailed analysis puts a burden on the security administrator to know and manage administrative credentials for each device to be scanned. This is overwhelming and time consuming for most mid- to large-size organizations. It is also impossible to manage for employee-owned devices. Not to mention it is yet another security weakness to store administrative credentials in a third-party solution.

US ProScan eliminates these problems by deploying a lightweight temporary host that scans from the device itself using the deployment infrastructure and systems management tools already in place in your organization. With US ProScan's patented cloud-based host scanning technology, millions of endpoints can be scanned simultaneously and return results quickly, even across large and highly segmented networks. On average, a full vulnerability scan for a Windows device takes about 60 seconds and approximately 30 seconds for Mac. Because the scanning is performed on each endpoint, it dramatically reduces the overhead on the network and allows each host to scan independently of any network device or appliance.

Remote and transient devices are blind spots

One of the biggest blind spots of most organizations is the ability to scan devices that are rarely on the network. Traditional vulnerability management solutions must be able to see the device on the network before it can be scanned. If the scan is started and the device disconnects from the network, then the scan results are lost.

With US ProScan, no matter when or where the device connects to a network or application, the device can be scanned using either a CLI scan or native app. And if the device disconnects or goes offline, the scan will still continue to run and the results will be made available the next time it comes back online.

Automated analytics for non-IT

US ProScan provides situational awareness as well as relevant and timely information that is consumable at all levels of the organization. US ProScan's data breach risk intelligence presents answers to the following questions in easy-to-understand graphics:

Where is my sensitive data and who has access to it?

Different organizations have different types of information. For retail organizations It could be payment data, for healthcare personally identifiable information, for many others its proprietary intellectual property such as design drawings, or chemical compounds or financial data.

No matter what a company holds as sensitive, the CISO and Board need to have confidence that they know where this data exists and which employees have access to it.

How can hackers and thieves get to my data?

CISOs also need to know how vulnerable data is to a breach. The vulnerability scan performs a complete assessment of the applications and operating system to determine any known vulnerabilities that exist and can lead to compromise. US ProScan's vulnerability database is comprehensive across all supported platforms including Microsoft Windows, Mac OSX and Linux as well as Android and Apple iOS.

What will it cost if I'm breached today?

The key to communicating breach risk effectively to the board and c-level executives is to use a universal language that is understood outside of IT.

US ProScan provides C-Level ready reporting that can communicate risk using dollars and helps business leaders throughout the organization have meaningful conversations about security priorities and actions.

Millions of endpoints can be scanned simultaneously with US ProScan's patented cloud-based host scanning technology.

CONCLUSION

Today's CISO must have solutions that translate security into business

A better architecture is needed to improve the speed, accuracy and relevance of data breach risk intelligence that CISOs can use to financially prioritize risk and to engage business leaders.

The US ProScan Data Breach Risk Intelligence Platform is a next generation security solution that provides relevant, actionable and timely intelligence to help organizations understand the various internal and external risks that can lead to a data breach. The results are a clear view of total risk posture, evidence of improvement, and connection to business outcomes.

Some specific benefits include:

Total risk posture exposed

With this information, total data breach risk exposure can be used by the Board and CFO to assess the business impact of a significant breach. They can also use it to budget security resources, and to take the guesswork out of cyber insurance.

Divisions made accountable

The risk contribution of each division, team or even individual can be measured. US ProScan calculates a security number for each device and financially prioritizes them. At a glance security teams can identify which individual assets are the highest dollar risk and why, and then take action on these first.

Timely data for decision-making

CISOs may be called on to give an executive briefing at any time. With the US ProScan Risk Intelligence Dashboard, they can have timely, actionable data ready to be presented.

Trends and evidence

US ProScan's trend charts indicate the overall cyber health of an organization. They provide proof of whether your policies and actions are successfully reducing the dollar liability -- or make an argument for more resources.

US ProScan

BUSINESS TECHNOLOGY SOLUTIONS

USProTech.com

DATA BREACH RISK INTELLIGENCE