Stratecast | FROST & SULLIVAN

Missing Critical Patches: A Cybersecurity Epidemic

Endpoint Security Hygiene Practices Fail to Keep Up with IT Priorities

A Frost & Sullivan White Paper

www.frost.com

Michael P. Suby

50 Years of Growth, Innovation and Leadership

Introduction 3

An Executive-level Survey 3

Priorities 3

Confident Up to a Point – Number of Endpoints 4

Prevention, Detection, Response: Confidence Wanes 5

Prevention through Scanning: Not a Reassuring Report Card 5

Prevention through Updating and Patching: Far from Uniform 5

The Basics in Endpoint Security Hygiene Need to Improve 6

The Last Word 6

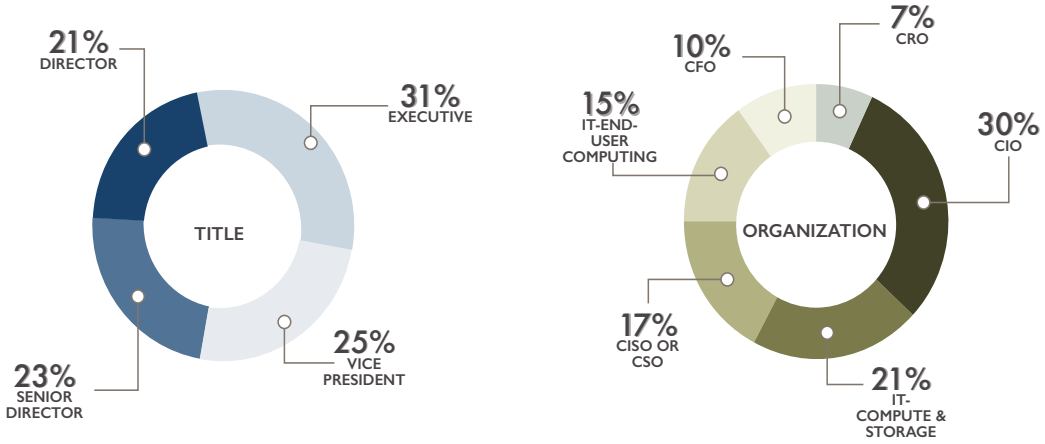
INTRODUCTION

IT security leaders know their companies' endpoints, PCs, and servers are continuously targeted by hackers. They also agree following best practices in endpoint security hygiene is instrumental in reducing cyber incidents. However, our 2017 survey of IT security leaders points to a situation where most are concerned about their actual practices in endpoint security hygiene. Fortunately, most also acknowledge they need to improve.

When it comes to identifying their top priorities, IT security leaders are clear: they want to reduce the frequency and severity of data breaches; streamline regulatory compliance; and maintain business continuity. When it comes to identifying and executing upon the security hygiene best practices required to deliver on these priorities, things begin to get murky. Our 2017 survey of IT security leaders reveals a situation in which most respondents express concern about their security hygiene practices and waning confidence in the ability of existing tools to help them improve. Read on for more about what we learned, plus five recommended action items you can take today to address these issues.

AN EXECUTIVE-LEVEL SURVEY

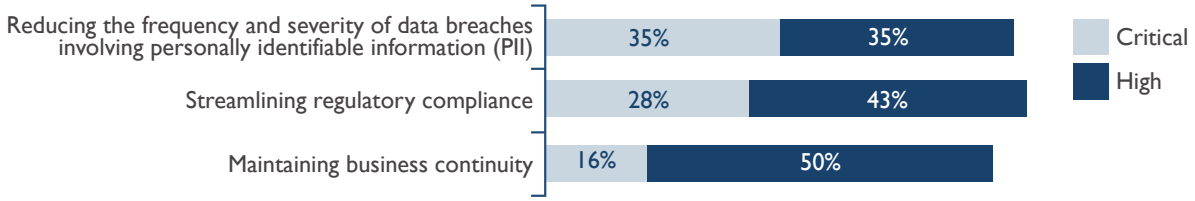
Our selection of 200 North America-based survey participants was exclusive: only individuals with direct decision-making authority (81% of survey) or strong influence on decisions (19%) pertaining to endpoint protection and security hygiene were included in the survey. All survey participants have a title of director or above and are members of organizations responsible for endpoint management and/or endpoint security. The percentages shown in this report reflect the percent of survey participants unless otherwise noted.



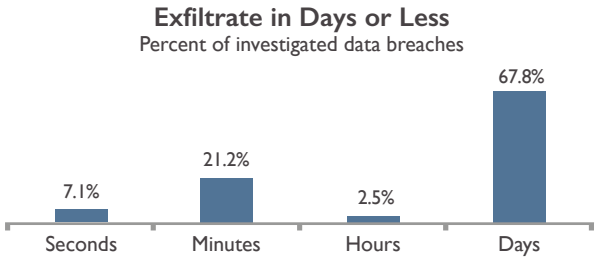
All survey participants are employed in companies with 2,000 or more employees, and management of endpoints is conducted primarily by internal staff (only 5% outsource management of 75% or more of their endpoints). Finally, the survey participants are from a broad range of industry verticals with the greatest percentages of respondents representing Manufacturing and Distribution (25%); Banking, Insurance, or Finance (19%); and High Tech or Information Technology (14%).

PRIORITIES

In our survey, the following IT security priorities were selected as critical or high by the majority of respondents:



These priorities, particularly the top two, are not surprising when weighed against sobering, time-measured statistics on data breaches. First, as data breach investigations compiled by Verizon[1] demonstrate, ***data exfiltration starts within days of network or endpoint compromise.***



Counteracting post-compromise data exfiltration first requires detection. Disconcerting, ***elapsed time from compromise to detection is measured in months***. According to the Ponemon Institute,[2] the mean time to identify is 201 days.

Once detected, more time is required for containment. According to Trustwave's[3] data breach forensics, ***the time to implement containment efforts after detection ranges from one day (median time for internally detected data breaches) to four weeks (median time for externally detected breaches).*** As common with data breaches, the majority (59%) of the data breaches included in Trustwave's analysis were externally detected.

Taking steps to shorten detection and containment times is understandably justified, but so is lessening the potential of being compromised. This is where endpoint security hygiene plays a crucial role.

CONFIDENT UP TO A POINT – NUMBER OF ENDPOINTS

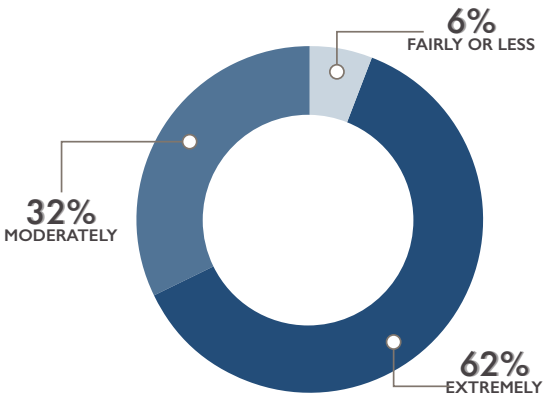
The first step in security hygiene rests on understanding the endpoints (i.e., the assets under attack). In this regard, the majority of survey participants are very confident that they know how many endpoints exist in their companies. Still, ***more than one-third acknowledges the likelihood of unaccounted endpoints.***

Also, few of the survey companies rely on a single approach to create and maintain an inventory of endpoints. The most popular approaches are:

72% - Conduct a physical inventory or sample endpoints routinely

71% - Have an automatic means for endpoints to check-in routinely

CONFIDENT ON EXACT NUMBER OF ENDPOINTS



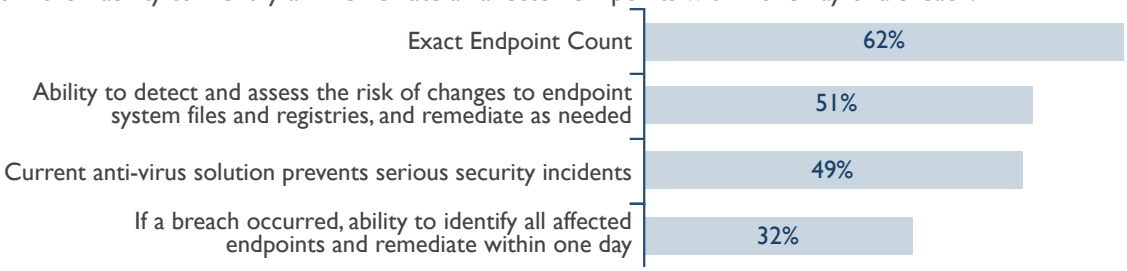
We question whether having multiple inventory approaches lulls executives into a false sense of confidence. For example, might one approach merely confirm the results of another, rather than be a fully independent and alternative approach to creating and maintaining an endpoint inventory? Additionally, inventory approaches based exclusively on physical attributes (e.g., serial numbers) will undercount virtual endpoint instances—servers and desktops. Similarly, if a rogue department were to stand up a virtual server without IT approval, would that server be identified? Furthermore, would the security practices applied to "shadow IT" virtual servers be as disciplined as servers known and directly managed by IT? Most likely, the answers are no. And, as we show in the next sections, endpoint operating systems and applications, more than the number of endpoints, is where security confidence wanes and concern intensifies.

Add to these scenarios the oft-cited "weakest link" risk: hackers may only need to locate and compromise a single endpoint. Given the increasing availability of commercialized hacking tools and services, the ability of a hacker to indiscriminately cast a wide net is not only economical, but also effective (if one approach does not succeed, try another).

[1] *Verizon 2016 Data Breach Investigation Report*
[2] *2016 Cost of Data Breach Study: Global Analysis*
[3] *2016 Trustwave Global Security Report*

PREVENTION, DETECTION, RESPONSE: CONFIDENCE WANES

If IT executives appear over-confident in their ability to identify the number of endpoints on their networks, confidence levels start to wane when it comes to evaluating prevention (effectiveness of endpoint anti-virus), detection and risk assessment (detecting risky system file and registry changes), and response (completeness and speed in responding to a detected data breach)[4]. Most notable in the chart below, less than one-third of survey participants said they are confident in their ability to identify and remediate all affected endpoints within one day of a breach.



PREVENTION THROUGH SCANNING: NOT A REASSURING REPORT CARD

Preventing security incidents is also dependent on visibility into the state of security configurations, existence of software vulnerabilities, and file integrity assessment. Lacking visibility into any or all three of these attributes elevates the risk of compromise.

Scanning for these attributes is considered a suitable approach. ***But as our survey revealed, scanning is neither comprehensive (all endpoints) nor continuous for most companies.*** Specifically, more than half of endpoints are not scanned or only scanned periodically for:

- Security configurations – 56% of survey participants
- Software vulnerabilities – 45%
- File integrity – 38%

Correspondingly, survey participants' views on the effectiveness of their companies' current scanning practices are not reassuring:

- 68% classify their current scanning practices for servers as ineffective
- 42% classify their current scanning practices for PCs as ineffective

PREVENTION THROUGH UPDATING AND PATCHING: FAR FROM UNIFORM

Patching software for critical security patches is a best practice in endpoint security hygiene. Again, as our survey demonstrates, IT security leaders have material doubts and concerns. ***With regard to installing critical OS security patches, 79% of survey participants said they are either "extremely" or "moderately" concerned that patches are missing from their endpoints.***

We also asked our survey participants for their top two reasons why critical OS security patches were not being installed on all of their endpoints or installation is significantly delayed. Aside from application incompatibility concerns, the other reasons point to deficiencies in endpoint security hygiene tools and circumstantial restraints:

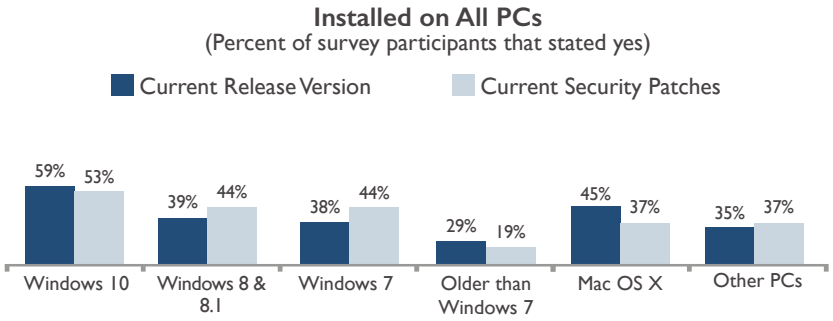
54% - Application incompatibility
41% - Lacking systematic means to install critical patches across all endpoints
29% - Lacking available IT resources to oversee patch installations
27% - Endpoints are offline for extended periods of time
24% - Incomplete visibility on which endpoints need which patches

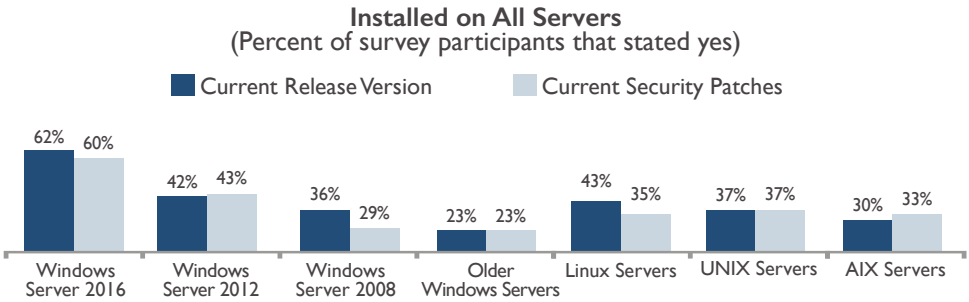
Further complicating efforts to practice good endpoint security hygiene is the lack of uniformity in endpoint environments and the number of endpoint security hygiene tools. Endpoint populations are highly diverse for all but a very small percentage of the surveyed companies. In fact, the majority of the surveyed companies have populations that span four or more operating systems.

58% - Have PC populations running 4-6 different operating systems
55% - Have server populations running 4-7 different operating systems

[4] Note, we did not request survey participants to differentiate based on breaches detected internally or externally.

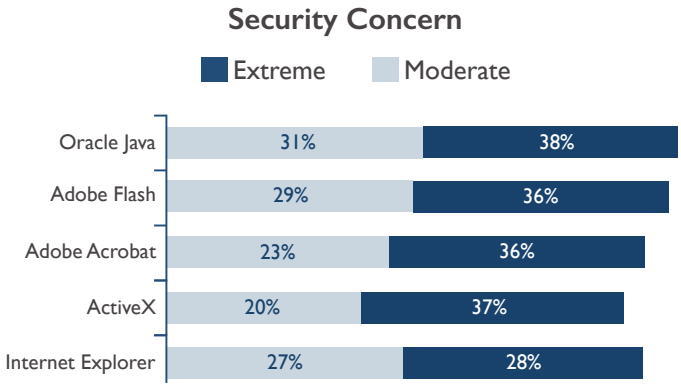
Overall, as OS diversity increases, currency in OS release version and security updates decreases. Additionally, as OS versions age, currency for endpoints running the same OS declines. This dynamic is illustrated in the following two charts for PCs and servers, respectively. Even with the newest versions of Windows—Windows 10 for PCs and Windows Server 2016—only slightly more than a simple majority of surveyed companies claim to be current in release version and security patches for all the endpoints running these latest OS versions.





Diversity does not end with endpoint populations. The survey results indicated companies have multiple endpoint security hygiene tools; ***41% state that they have four or more tools used in support of endpoint security hygiene.***

In addition to concerns about currency in OS release version and security patches, the majority of the survey participants also expressed extreme or moderate levels of security concern regarding high-use applications, as shown in the following chart.



THE BASICS IN ENDPOINT SECURITY HYGIENE NEED TO IMPROVE

The basics of endpoint security hygiene matter. By basics, we mean visibility into the endpoint security foundation and certainty in taking actions that improve that foundation (e.g., patch and update). Without effectiveness in these basics, endpoints are more vulnerable to attacks, are compromised with greater frequency, and, from a compensatory perspective, there is greater reliance on cybersecurity defenses to thwart attacks aimed at exploiting a weak foundation.

The basics in security hygiene have significant room to improve:

- More than one-third of survey participants acknowledge their organizations do not know with certainty how many endpoints exist on their networks;
- Nearly half of survey participants are, at best, moderately confident in their organizations' ability to detect risky system file and registry changes;
- More than half of survey participants categorize their current endpoint security scanning practices as ineffective; and
- Nearly 80% of survey participants are extremely or moderately concerned that critical OS security patches are not installed or that installations are significantly delayed.

THE LAST WORD

Acknowledging a problem exists does not, by itself, solve the problem. IT security organizations need to take steps to improve the basics of security hygiene. To move forward, organizations should objectively rate their current security hygiene tools based on what they accomplish and what they do not accomplish. This rating will produce a priority list of the attributes to seek in new or replacement security hygiene tools and what these tools should accomplish.

While every company and every IT security organization is unique, we recommend IT security organizations consider security hygiene tools that accomplish the following:

- Create and maintain a complete inventory of endpoints;
- Curate the entire software stack of each endpoint (software installed and each software's release version and patch level) and each endpoint's security configurations;
- Trigger high-fidelity, real-time alerts on risky changes to the endpoint software and changes to system files and registries;
- Across all endpoints, orchestrate administrative changes to endpoint software (e.g., upgrading and patching) with speed, precision, and irrefutability; and
- Seamlessly integrate with cybersecurity technologies, such as vulnerability management, security information and event management (SIEM), network defenses, and endpoint detection and response (EDR), in order to elevate the security efficacy of the interconnected system.

In the finite world of IT security resources—personnel and budgets—the preferred security hygiene tool should also reduce the number of hygiene tools, lessen support effort in compliance reporting, and automate repetitive processes. Once the new tool is operational, IT security organizations that were once struggling with endpoint security hygiene will move from the low-confidence/high-concern responses contained in this survey to high confidence/low concern.

Michael P. Suby
VP of Research
Stratecast | Frost & Sullivan
msuby@stratecast.com

ABOUT STRATECAST

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.

CONTACT US

For more information, visit www.stratecast.com, dial 877-463-7678, or email inquiries@stratecast.com.

NEXT STEPS

- **Schedule a meeting with our global team** to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.
- Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.
- Visit our **Digital Transformation** web page.
- Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

SILICON VALLEY
3211 Scott Blvd
Santa Clara, CA 95054
Tel 650.475.4500
Fax 650.475.1571

SAN ANTONIO
7550 West Interstate 10
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

LONDON
Floor 3 - Building 5,
Chiswick Business Park
566 Chiswick High Road
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
3211 Scott Blvd
Santa Clara CA, 95054