IDC PERSPECTIVE

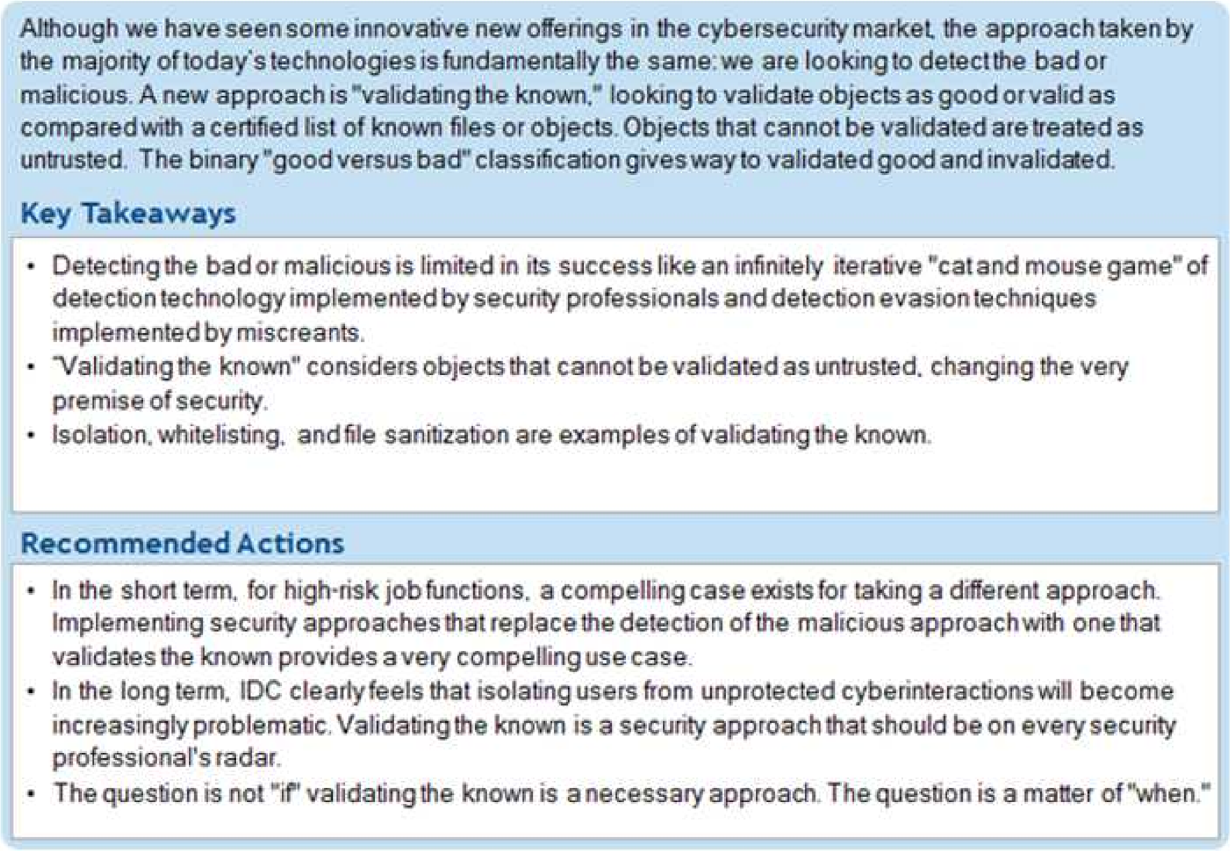
Validating the Known: A Different Approach to Cybersecurity

Frank Dickson Robert Ayoub

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Validating the Known — A Different Approach to Cybersecurity



Although we have seen some innovative new offerings in the cybersecurity market, the approach taken by the majority of today's technologies is fundamentally the same: we are looking to detect the bad or malicious. A new approach is "validating the known," looking to validate objects as good or valid as compared with a certified list of known files or objects. Objects that cannot be validated are treated as untrusted. The binary "good versus bad" classification gives way to validated good and invalidated.

Key Takeaways

- Detecting the bad or malicious is limited in its success like an infinitely iterative "cat and mouse game" of detection technology implemented by security professionals and detection evasion techniques implemented by miscreants.
- "Validating the known" considers objects that cannot be validated as untrusted, changing the very premise of security.
- Isolation, whitelisting, and file sanitization are examples of validating the known.

Recommended Actions

- In the short term, for high-risk job functions, a compelling case exists for taking a different approach. Implementing security approaches that replace the detection of the malicious approach with one that validates the known provides a very compelling use case.
- In the long term, IDC clearly feels that isolating users from unprotected cyberinteractions will become increasingly problematic. Validating the known is a security approach that should be on every security professional's radar.
- The question is not "if" validating the known is a necessary approach. The question is a matter of "when."

Source: IDC, 2017

SITUATION OVERVIEW

Let's face it. The 2017 cybersecurity reality is bleak, and the task of guarding our cyberassets is increasingly difficult. We can attribute this reality to four key trends:

- **The sophistication of cybermiscreants is growing rapidly.** From massive scale Internet of Things (IoT)-based DDoS attacks to ransomware, cybermiscreants are becoming even more clever. These attackers are motivated by the increasingly large "pay days" providing a return on their efforts. Cybercrime has paid handsomely as of late with ransomware attacks alone netting over $1 billion in 2016.
- **The perimeter has died.** It is safe to consider the impenetrable network perimeter officially dead, as our data, applications, and devices cannot predictably be found in the networks that reside behind perimeters. Today, compute, application, and data resources reside on-premises or in the cloud or simultaneously in both. These resources are accessed from workstations, PCs, Macs, smartphones, tablets, and a potpourri of IoT devices like printers. Cybersecurity professionals have been tasked with protecting and securing corporate resources and maintaining compliance with a host of standards such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the National Institute of Standards and Technology (NIST), and the ISO 27000 family of standards.
- **Security tools are proliferated.** As the number of cybersecurity challenges grew, so did the number of security point products offered by security companies to address those challenges. IBM cites an example of one client having 85 different security tools from 45 different vendors. Operation, maintenance, and employee training become an issue in such environments.
- **Qualified information security professionals are scarce.** By 2019, (ISC)^2 predicts that the shortfall of qualified security professionals will exceed 1.5 million. "Pushing security tasks onto traditionally nonsecurity IT professionals and leaving some security tasks undone or suboptimally completed are the larger, unseen outcomes." In other words, the problem is getting worse.

A New Approach

Although we have seen some innovative new offerings in the cybersecurity market, the approach taken by the majority of today's technologies is fundamentally the same approach: we are looking to detect the bad or malicious. This approach is limited in its success, like an infinitely iterative "cat and mouse game" of detection technology implemented by security professionals and detection evasion techniques implemented by miscreants. McAfee describes the phenomenon as the Grobman Curve of Threat Defense Effectiveness. The only way to escape the continual "cat and mouse game" is to approach the problem differently, fundamentally redefining the approach.

One such new approach is "validating the known." Fundamentally, the approach takes a different tact, looking to validate objects as good or valid as compared with a certified list of known files or objects. Objects that cannot be validated are treated as untrusted, changing the very premise of security. The binary "good versus bad" classification gives way to validated good and invalidated.

Isolation

A variant of the "validating the known" approach is browser isolation. Isolation accepts that it may be impossible to 100% validate objects, taking a "protect first, expect the worst" perspective. As a result, objects that come from invalidated and/or untrusted channels such as the internet are kept sequestered, isolated in virtual machine environments with interaction limited to graphic rendering to a viewing device. Much like viewing the activity behind a glass window of a clean room, interaction with the outside world is limited to visual stimuli, regardless of whether the isolation environment is on a server, in the cloud, or on an endpoint.

Several attributes should be considered when comparing solutions. Although the viewing is done from behind a glass wall (or any other metaphor), the user experience should remain to be demonstrably similar to a native browsing experience. Also, solutions use different virtualization environments including Windows virtual machines and Linux containers. Finally, solutions will vary based on where the isolation takes place, on the endpoint or in a remote location, and also whether there is a need to install a client on the endpoint.

Whitelisting

To help to safely navigate the internet, blacklisting and whitelisting, variants of the "validating the known" approach, have long been used. Blacklisting validates a list of known bad sites and blocks them. Blacklisting is a fairly simple and reasonable approach, but it is limited, given the realities of today's internet. Blacklisting falls prey to the cat-and-mouse game. Hackers dynamically spin malicious sites up and down; many malicious sites will exist for less than 24 hours, making the maintenance of a complete, vetted blacklist impractical.

The whitelisting approach is the opposite of blacklisting, validating known good sites. Whitelisting is a much better approach as it is easier to identify and validate known good sites. It is also much easier to identify the sites that will command the majority of internet traffic. However, whitelisting suffers from a similar limitation as blacklisting in that it is challenging to create a truly comprehensive list. Even if the whitelist covers 99% of traffic, it means that one in 100 requests get blocked and results in a help desk ticket. In an organization of any size, an impractical and unproductive inventory of help desk tickets is created. Thus the only list that is truly up to date is the list of annoyed users. In addition, many commonly whitelisted sites connect to many background sites over which the administrators have no control. Many of those sites are running old vulnerable versions of code, which make the primary site vulnerable. As a result, traditional whitelisting becomes impractical to maintain.

File Sanitization

The primary attack vector today is email. The preferred attack instrument du jour is weaponized files with embedded malware or malicious code/scripts. We give these types of attacks the moniker of "exploit." Taking advantage of a vulnerability in a browser or in Microsoft Word to launch PowerShell commands on a remote endpoint to take control of the device would be representative of an example of exploit. Exploits are challenging for signature-based defenses as there is often a lack of any discernible malware and the exploit often targets an unknown vulnerability.

Exploits are especially vexing as they are sophisticated attacks that can be used by the unsophisticated. Exploits are typically implemented using exploit kits that reside on web servers. An exploit kit identifies software vulnerabilities on endpoints and then uploads and executes malicious executables to the endpoint in an automated fashion. Creating an exploit kit requires sophistication, but using an exploit kit does not, as easy-to-use packaged exploit kits are readily available on the dark web for as little as $500 per month. As you might expect, exploit kits are currently "the rage."

File sanitization examines common file types such as PDF, Word, Excel, and image files, looking for unknown or nonconforming components with deep file inspection against the manufacturer's file design specification. Unknown components are typically then removed, nonconforming structures are corrected, and a clean file is regenerated. Corrupted or seriously nonconforming files can be quarantined.

IDC believes that a new generation of isolation, whitelisting, and file sanitization vendors hold the possibility of significantly improving the block rate of attacks. The sections that follow provide details on a new set of vendors offering solutions.

Sample Vendors

Authentic8

Authentic8 is a company born from Postini, an email security company purchased by Google. Authentic8 takes a different approach to browser isolation, offering a secure yet virtual browser. Silo runs on Authentic8's server and isolates all web code in a secure, remote container giving users a benign display of the web content. Devices connect via SSL, and data is exchanged via a proprietary remote display protocol. All content executes in the container, and zero web code reaches the device.

Instead of being offered as an application, the browser is delivered as a service. The browser is built to allow users to connect securely from any device or from any network. In addition, the browser has policies and controls embedded within it. IT controls the browser that employees use, regardless of where they are. IT can also control cloud-based work assets by binding credentials to its Silo profile.

Silo can be used in different modes:

- A one-time use disposable browser for personal browsing that doesn't expose your firm
- Authenticated access to business apps with device-specific rules and data exchange policies
- Spoofed identity and geolocation with code analysis tools for forensic researchers
- Integrated, encrypted cloud-based storage for individuals and groups

Silo gives admins the ability to configure and provision web-based accounts to users or groups. Admins can control individual credentials, manage shared credentials across teams, or allow users to control their own. Revoking access is even simpler. There is a kill switch for web data when personnel changes.

The Authentic8 offering goes beyond browser isolation, including a data security component. The Silo platform includes enterprise policy controls that can allow or restrict key browser functionality based on business requirements or user roles. Policies remain intact no matter what device or what network is being used. Silo policies enable or restrict file uploads, downloads, printing, and copy-paste operations. Also, all user activity is logged with a customer-managed encryption key so your audit and remediation processes are intact.

For more information on this vendor, visit **www.authentic8.com**.

Bromium

Bromium Secure Platform provides isolation environments for secure web browsing as well as for document editing and operation of other host-based applications. As opposed to other approaches that create a single virtualized "endpoint" environment in the cloud or on the endpoint, Bromium creates hardware-isolated micro-VMs. Each application is launched within its own micro-VM. The micro-VMs live on the endpoint, eliminating latency issues and securing every user task such as visiting a webpage, downloading a document, or opening an email attachment. Each application task runs in its own micro-VM, and all micro-VMs are separated from each other using hardware enforcement and thus not susceptible to kernel exploits.

The Bromium offering satisfies two uses cases. The first is isolation for secure internet browsing or secure file editing. The second is visibility, monitoring endpoint activity for signs of malicious behaviors.

Bromium Secure Browsing isolates users from web-borne threats and browser exploits with hardware-enforced micro-virtualization. Each individual browser tab is isolated from all other tabs, the host PC, the network, and the file system. The micro-VM container for each tab is disposed at the end of the tab session, and new micro-VMs are spun-up when new tabs are launched, invisible to the end user. Bromium Secure Browsing supports Chrome, Internet Explorer, and Firefox. In addition, Bromium supports trusted websites, allowing access outside of the micro-VM at the choice of the administrator. System resource impact is kept to a minimum, often times improving machine performance with the way in which Bromium performs VM scheduling and VM density management.

Bromium Secure Files is practically an identical service to Secure Browsing, except the application in the micro-VM is a file-centric application instead of a browser. File activity takes place within a micro-VM, protecting against malicious document-based attachments regardless of the source such as phishing email or internet download. Typical application types include Microsoft Word, Adobe PDFs, Microsoft PowerPoint, and other productive applications.

For more information on this vendor, visit **www.bromium.com**.

Citrix

As part of its XenApp and XenDesktop, Citrix offers Secure Browser. Secure Browser is a virtual browser that enables IT to deliver secure remote access to web and SaaS applications without endpoint configuration. Users can open web and SaaS business apps in their local browser simply by entering or clicking on a specified URL. This opens a Citrix Receiver for HTML5 session that displays the web application in the predefined virtual browser, integrated into a new tab in the local browser without the need for a VPN.

Citrix Secure Browser centralizes the applications and data within the hardened datacenter. Only screen updates, mouse clicks, and keystroke commands cross the network to the user's endpoint device. No data resides on the device or in the local browser cache, and nothing is left behind when the network connection is terminated. Granular access policy enforcement eliminates VPN holes and reduces the risk of data loss or intrusion through unsecured connections.

Secure Browser is available as a hosted service available from Citrix Cloud. Citrix manages all the infrastructure and servers to deliver secure remote access to websites on-premises or from the cloud.

For more information on this vendor, visit **www.citrix.com**.

Cyberinc

Founded in 2012, Spikes Security offered a web malware isolation system. After a Spikes Security acquisition, Cyberinc was formed by merging Spikes Security with Aurionpro's security division and is a wholly owned subsidiary focused on enterprise security.

The Cyberinc offering is a malware isolation appliance family, which isolates original web content outside the network, away from endpoint devices, then transforms that content requested by a user into an optimized, encrypted, and proprietary data format before it ever makes it into the network or onto the endpoint. This content is in a benign format that malware does not recognize and cannot exploit, rendering it harmless to the endpoint. For example, attackers using approaches like steganography to conceal malware within images or files are ineffective. When Isla is employed, endpoints remain isolated from the internet. Appliances are available in a range of configurations supporting between 90 and 1800 concurrent users. Isla supports Windows, Mac, and Linux with a HTML5-based "zero client," which is automatically "pushed" into the endpoints' current web browser. The Isla solution includes the Isla Control Center, which provides IT security managers with the tools required for fast deployment and management of Isla appliances across the enterprise.

For more information on this vendor, visit **www.cyberinc.com**.

Ericom Software

Ericom Shield is a proxy-based solution that uses whitelisting and blacklisting policy definitions to determine when to activate a virtual browser. It interfaces with any industry proxy or uses its own built-in proxy functionality. Ericom Shield is a clientless solution, requiring no installation on the endpoint. It can be deployed on-premises, in the cloud, or as a hybrid solution.

By default, every link or browsing session that is not categorized (whitelisted or blacklisted) will power up a dedicated container running a remote virtual browser. This ensures that all untrusted web content executes remotely in an isolated and disposable Linux container in the DMZ/cloud, away from the endpoint. Web content is rendered in real time, delivering a safe visual stream to the user's local browser without executing any code on the endpoint, providing a seamless and native browsing experience. At the end of each session or after a predefined idle period, the remote container is discharged, eliminating any malware that may have been there.

Ericom Shield comes pre-integrated with file sanitization technology, eliminating the need for third-party integrations. While browsing, downloaded files are scanned and sanitized in the background without impacting user experience or file functionality. Once the file has been approved for usage, it is downloaded to the endpoint.

For more information on this vendor, visit **www.ericom.com**.

Fireglass (Symantec)

In July of 2017, Symantec entered into an agreement to buy Fireglass. Fireglass provides a browser isolation offering. Website and email content and attachments are executed within a separate environment, delivered as a fully interactive visual stream to the user. No website content reaches the user. It's available as a cloud service, as on-premises software, or in a hybrid model. The Fireglass acquisition provides Symantec with the products that integrate immediately with its proxy-based secure web gateways along with the team and intellectual property to strengthen its secure web gateway and email protection offerings.

Symantec CEO Greg Clark said, "Integrating Fireglass' isolation technology with Symantec's existing endpoint, email, and secure web gateway solutions could reduce security events by as much as 70%, while virtually eliminating advanced threats spread by web browsing or email content. Isolation will become a core component in the design of cyberdefense architectures for the cloud generation that face the reality of an encrypted internet and the crisis inherent in email and web-delivered attacks. The ability for the security team to take an aggressive stance on unknown websites and questionable attachments without causing chaos for a company's users and IT help desk is now a reality. Isolation is a key element of securing the cloud generation and is even a productivity gain for both the end user and security operations center."

For more information on this vendor, visit **www.fire.glass**.

Glasswall

Glasswall provides document sanitization, integrated with existing email solutions or document-based web applications, ensuring that only the "known good" will enter or leave the business environment within documents or email attachments. Glasswall breaks down documents and email attachments to their component parts before regenerating a new file that complies entirely with the manufacturer's original design standards.

Glasswall's software operates across three distinct phases: inspection, remediation, and delivering a secure, clean, and compliant file to the user. Inspection breaks down each file to its component parts and conducts structure conformance checks against the respective document manufacturer's design or ISO standard. Glasswall also checks the functional elements of documents that could be considered a risk factor such as Macros, JavaScript, embedded URLs, embedded malformed images, active content, and AcroForms. Glasswall then regenerates a new, compliant, and clean version of the original file, allowing users to interact with the file as they normally would – editing, saving, and sharing the document with complete confidence that the document is always safe.

For more information on this vendor, visit **www.glasswallsolutions.com**.

Light Point Security

Light Point Security was founded in 2012 by two former National Security Agency (NSA) cybersecurity veterans to address the security risks imposed by web browsers and the ineffectiveness of traditional detection-based security methods. Light Point Security provides remote isolated browsing. The company's product, the Light Point Web Full Isolation Platform, is a full isolation remote browsing platform that integrates with existing browsers. The product's unique architecture ensures that malicious web content never reaches enterprise endpoints.

For more information on this vendor, visit **www.lightpointsecurity.com**.

Menlo Security

Menlo Security provides a cloud-based (either public or private) isolation environment that protects users from web, document, and email threats. The Menlo Security Isolation Platform (MSIP) executes and contains the user's web session and all active content (e.g., Flash) away from the endpoint. Web requests are proxied via the MSIP, which accesses the web on the user's behalf and executes the user's session. The MSIP can be deployed standalone or in conjunction with existing web security gateways, next-generation firewalls, network sandboxes, or other security systems. It also integrates with an organization's mail servers to provide protection against spear phishing and other email attacks.

Menlo Security's Adaptive Clientless Rendering (ACR) technology provides the connection from the user's session running in the MSIP to the user's native browser. ACR technology requires no endpoint software or plug-ins and delivers a native user experience.

For each type of web content, the ACR engine selects the optimal encoding and transport mechanism for delivery to the user's browser. For example, dangerous content such as Flash is executed in the MSIP and then delivered as a hi-fidelity, interactive experience in the user's browser. In all cases, the user's browser receives nonexecutable, malware-free content that renders naturally and preserves the user's native experience. Benefits of the ACR approach include the following:

- Works with the user's native browser (IE, Chrome, Safari, or Firefox), meaning no requirement for any software on the end-user device (i.e., no thin client, replacement browser, plug-in, etc.)
- No pixelation, choppy scrolling, or other visual artifacts common with "screen scraping" technologies like VDI
- Preservation of native browser functionality such as cut and paste, printing, and so forth
- Native support for browser extensions
- Enables input restrictions on web forms to prevent credential theft

The Menlo Security Isolation Platform was architected from the ground up as a multitenant, elastic cloud service.

For more information on this vendor, visit **www.menlosecurity.com**.

Ntrepid

Ntrepid's secure anonymous browser, referred to as Passages, establishes a web browser in a virtual environment on the endpoint. The browser "walks, talks, and acts" like a normal browser; however, it is hardened, completely isolating the browser from the rest of the user's system to manage high-risk web browsing applications on endpoints with a heightened need for security. Every new session is established based on a clean image, which is subsequently discarded at the end of a session.

The Passages platform provides additional benefits to strengthen the security efficacy of the isolation environment. All user and device identifying attributes are removed so that the originating source cannot be known. Downloaded files are placed in cloud-based file storage with integrated scanning, further protecting the host device from malicious payloads in the isolation environment. Administrative and reporting tools integrate with account management, deployment, and analytics platforms.

For more information on this vendor, visit **www.ntrepidcorp.com**.

Terra Privacy

Terra Privacy has taken a very different approach to validating the known. Instead of focusing on files or websites, Terra Privacy focuses on known connections.

Terra Privacy has implemented a clever application of dynamically generated whitelisting. Dynamically generated whitelisting takes a fundamentally different approach to static whitelisting. Dynamically generated whitelisting begins with zero trust by default; essentially, there is no white list. A white list is dynamically generated based on activity. For example, if a person goes to myfavoritesportssite.com to check the scores for the local team, the only browser traffic that should be trusted is the traffic to the webpage itself as well as the content sites that the webpage needs to load. All other browser traffic should remain untrusted (and therefore blocked). Dynamic whitelisting therefore creates a list in real time that includes myfavoritesportssite.com and all of its required connections. If the browser attempts to go anywhere else, that attempt is blocked. Determining whether the browser's unwhitelisted connection is malicious is irrelevant; it is simply blocked because it is unknown. The traditional cat-and-mouse game is avoided.

Terra Privacy uses dynamic whitelisting to address the problem created by the malicious use of Trojans. Both application and browser-based use cases are confronted.

To bypass traditional malware detection methods, Trojans often leverage a legitimate application to access the internet. Essentially, Trojans capitalize on weaknesses or vulnerabilities to make good applications do bad things.

Dynamically generated whitelists are uniquely effective against nonbrowser Trojans. For traditional applications like document processing or spreadsheets, an application may need to communicate with the developer of the application but likely not with any other entity. For example, Microsoft PowerPoint usually only needs to talk to Microsoft Corporation. Lotus Notes would traditionally only need to communicate to IBM. Thus, applications are permitted to communicate with the developer; all other connections such as injected Trojan command-and-control connections are blocked. Remember, the connection is not blocked because it is necessarily malicious; it is blocked because it is unknown.

Dynamically generated whitelists are similarly effective against browser-injected Trojans. Webpages often require connections to third-party sites. For example, many webpages pull content from Google AdWords to monetize sites with advertising. Hacker-injected Trojans leverage this use case to enable command-and-control connections. Terra Privacy leverages a dynamically created whitelist to solely permit connections to currently open webpages and their required additional connections. All other browser traffic remains blocked. Browser-injected Trojans are unable to connect to command-and-control centers, rendering the Trojan sterile.

For more information on this vendor, visit **www.terraprivacy.com**.

VMware

VMware offers a browser appliance. This virtual machine provides an isolated environment in which to browse the web using Mozilla Firefox. The Browser Appliance leverages virtual machine isolation capabilities to prevent malware downloaded in the browser from propagating to the normal desktop. The Operating System and Browser are encapsulated in a disposable virtual machine.

For more information on this vendor, visit **www.vmware.com**.

ADVICE FOR THE TECHNOLOGY BUYER

In a 2017 IDC FutureScape, IDC predicted the following:

> By 2020, 20% of endpoints will be protected by isolation environments in an effort to "validate the known," a construct where the binary "good versus bad" classification gives way to validated good or simply invalidated.

Clearly, the major threat vector is people, our people. Our enterprise employees are not unaware or uncaring, but our employees are hyperconnected. Interaction is a nature course of business. Knowing valid and legitimate emails and websites can be problematic, even for security professionals. Cybermiscreants are smart and clever. They continually find innovative ways to breach networks.

Many actions can be taken. Better security hygiene will help. Stronger forms of authentication are a plus. Stronger security defenses make a difference. However, in the end, a cat-and-mouse game ensues. Victory for the miscreant can occur if attacks are successful in 1 in a 100 tries, or even 1 in 1,000 tries.

Some job functions are especially problematic. Human resources, for example, open a number of unsolicited documents (resumes) as a natural course of the job function. Any one resume can include a weaponized exploit that breaches the network. Accounts payable and accounts receivable functions has a similar peril.

In the short term, for high-risk job functions, a compelling case exists for taking a different approach. Implementing security approaches that replace the detection of the malicious approach with one that validates the known provides a very compelling use case. In the long term, IDC clearly feels that isolated users from unprotected interaction will increasingly become a problem. Validating the known is a security feature that should be on every security professional's radar. The question is not "if" the approach is necessary. The question is a matter of "when."

LEARN MORE

Related Research

- *Fireglass, Skycure Acquisitions Crystallize Symantec's Move to Distributed Security* (IDC #lcUS42886617, July 2017)
- *Worldwide Security and Vulnerability Management Forecast, 2016-2020: Enterprises Continue Focus on Security Operations* (IDC #US41943616, December 2016)
- *Worldwide Security and Vulnerability Management Market Shares, 2015: Top Vendors Acquire and Integrate to Deliver Powerful, Flexible Platforms* (IDC #US42068716, December 2016)

Synopsis

This IDC Perspective discusses a new approach to cybersecurity: validating the known.

"Although we have seen some innovative new offerings in the cybersecurity market, the majority of today's technologies take fundamentally the same approach: we are looking to detect the bad or malicious. A new approach is 'validating the known,' looking to validate objects as good or valid as compared with a certified list of known files or objects. Objects that cannot be validated are treated as untrusted. The binary 'good versus bad' classification gives way to validated good and invalidated," according to Frank Dickson, research director, Security Products.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world"s leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA-01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.