WHITE PAPER

McAfee™ Together is power. | Bromium®

Defining a Modern Endpoint Security Stack

Redesigning endpoint security with the smallest footprint, lowest cost, and highest effectiveness

Table of Contents

Contents

Executive Summary

Despite record spending on cyber security, government agencies and enterprise organizations are not making significant headway in winning a battle against cybercrime.

As part of an ongoing modernization initiative, the U.S. DoD is evaluating security solutions that offer the smallest footprint, lowest costs, and highest effectiveness against cyber-attacks. The combination of containment (Application Isolation and Containment) and Endpoint Detection and Remediation (EDR) technologies provides the most comprehensive protection for the endpoint as well as High-Value Assets, along with the fastest breach response times. Two prominent enterprise security experts, Bromium and McAfee, have joined forces to deliver an integrated solution that approaches cyber threats from multiple angles, reducing the noise of false positive alerts, minimizing triage times, decreasing operational costs, and helping harden the entire security infrastructure against future attacks.

No single defensive solution can completely protect an organization from threats, but implementing a set of best-of-breed integrated tools, including Bromium Secure Platform, McAfee Active Response, and Bromium Protected App, gives you the greatest chance for success.

WHITE PAPER

Defining a Modern Endpoint Security Stack

Redesigning endoint security with the smallest footprint, lowest cost, and highest effectiveness

There are two major trends in today's cyber security. First, government departments and agencies appear to be losing the battle against advanced, targeted cyber-attacks. According to Gartner, worldwide cyber security spending is estimated to increase from $114 billion in 2018 to $170 billion by 2022[i]. At the same time, research shows that cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015[ii]. When comparing how much organizations spend on security vs. how much they are projected to suffer in damages, it is very clear that cybercrime costs far outpace security investments. The second trend, cyber-attacks are becoming increasingly threatening. According to the World Economic Forum, cyber-attacks are now ranked as the highest risk, globally, above asset bubbles, fiscal crises, and natural disasters. In the United States, they are even ranked higher than terrorist attacks[iii].

In a study conducted by Ponemon Institute, the average endpoint has at least seven different agents installed on it for IT management and security, with many of the security agents offering the same set of capabilities[iv]. Endpoint security is increasingly becoming more difficult and costly to manage, yet most organizations don't feel like they get adequate protection from their security stack. Surveys reveal that the inability of the existing security solutions to fully safeguard against threats is ranked as the highest pain point among organizations and agencies of all sizes, while the second highest-ranked issue is the sheer volume of false positives and security alerts that require triage. With this amount of noise, it is no surprise that threats go undetected for an average of 196 days before being discovered[v]. It's evident that cyber threats have evolved and have created the need to modernize traditional endpoint security; while protection is still important, it is no longer singularly sufficient because we need to continually protect, detect, correct, and adapt to an ever-evolving adversary.

The U.S. Defense Information Systems Agency (DISA) is at the forefront of cyber defense. The world's largest IT enterprise, the U.S. Department of Defense (DoD), is investigating containment (Application Isolation and Containment) and Endpoint Detection and Response (EDR) capabilities as part of a modernized security stack that provides the smallest overall footprint, lowest cost, and highest effectiveness against cyber-attacks.

The objective of this white paper is two-fold: To identify key use cases facing the broader DoD workforce and to highlight technologies that can deliver the best value to organizations looking to secure their assets against threats – known and unknown.

The following security technologies are reviewed in this paper:

- Application Isolation and Containment: Bromium
- EDR: McAfee
- Threat Intelligence Exchange (TIE)/Data Exchange Layer (DxL): McAfee
- High Value Asset protection: Bromium

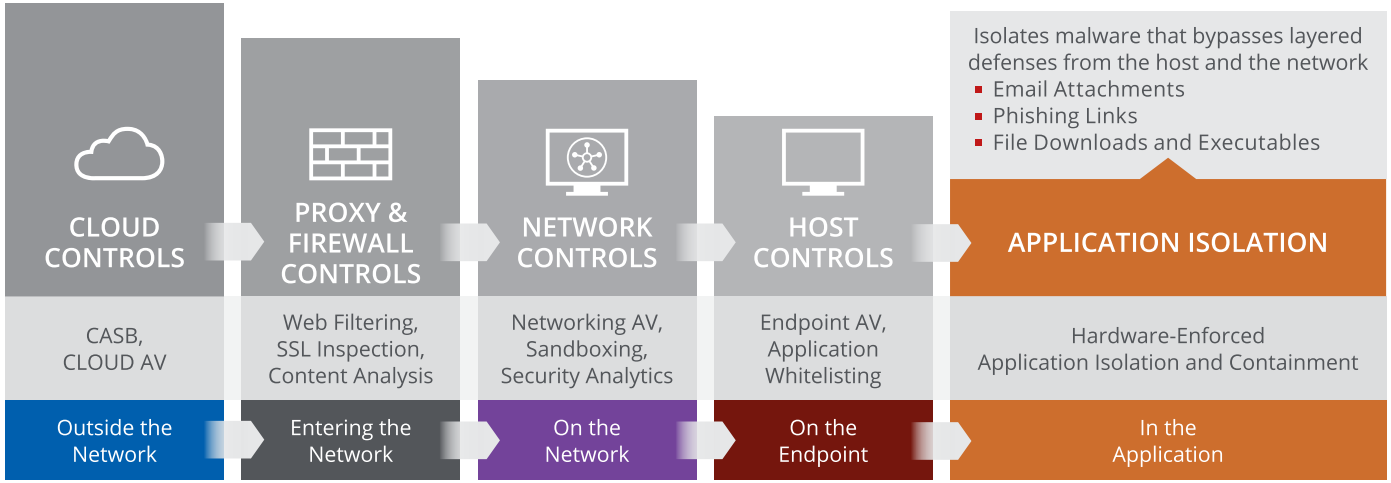

Figure 1: Application Isolation and Containment provides effective protection against cyber-attacks

How Threat-Actors Continue to be Successful

Attackers see applications—in particular email and browsers—as a favorite target, because they present the best chance of tricking users into clicking on links or attachments or installing software that infects their PCs, bypassing layered defenses.

Current tools are not able to offer reliable protection – 2017 saw a steady stream of major data breach incidents—such as Equifax and Deloitte—with significant implications for consumers, and potentially even national security.

The WannaCry and NotPetya ransomware campaigns showed us that cyber-threats are not all about data theft. WannaCry infected more than 250,000 endpoints in 150 countries in a matter of hours[vi], causing scores of National Health Service (NHS) Trusts in the UK to cancel patients' procedures and appointments.

NotPetya infiltrated OT networks, crippling supply chains in manufacturing, transportation, utilities, and other industries. The impact was felt across the globe, with Danish shipper Maersk[vii] and FedEx[viii] each revealing losses of up to $300 million, and a British consumer company, Reckitt Benckiser losing as much as $135 million in revenue due to production disruptions[ix].

Favored Attack Vectors:

For global enterprises and the DoD, the scale of the problem is the same. Endpoints are distributed around the world, supporting ashore, afloat, air, and space operations. These systems are needed for real-time decision making and must be resilient to cyber-attacks to ensure business and mission continuity. Even with all the of advances in layered defenses, threat-actors continue to be successful with the following primary attack vectors:

- **Malicious Email Attachments:** According to the 2018 Verizon Data Breach Report, email is by far still the most effective attack vector, with 92% of infections originating from email[x], 47%[xi] of which are unique, never-before-seen, polymorphic or zero-day malware instances.
- **Malicious Links:** When using social engineering, attackers have a 46% success rate to entice users to click on web links in email[xii]. Further, it's estimated that 3 out of 7 organizations had to remediate file-less attacks last year[xiii].
- **Malicious Downloads:** In the last year, malvertizing has increased exponentially, impacting 145 million US consumers[xiv]. Even though 88% of organizations restrict their end users from using uncategorized websites[xv], legitimate websites are often used to trick users into installing malware-ridden updates – Adobe Flash installers are among the most common.

Types of Attacks that Threat-actors are Exploiting:

Attack Types and Risks	Scope of the Problem and Prevalence
Malware-based intrusions	Every day over 350,000 new variants of malware are released, with new species of malware being generated every 4.2 seconds. On average, intruders can start moving laterally within one hour of malware being installed on an endpoint[xvi].
File-less intrusions	File-less attacks using compromised credentials or malware that runs in memory continue to increase in popularity for nation-states and threat-actors alike; they account for 39% of all attacks, as observed by CrowdStrike[xvii].
Software vulnerabilities	A recent study shows that most (57%) of breached organizations attributed the breach to a vulnerability for which a patch was available[xviii]. It takes an average of 67 days to patch computer systems, even after specific vulnerabilities have been identified, patches made available, and patching plan put in place. This does not account for legacy infrastructure and systems where patching is not an option, presenting a sizable problem for the U.S. DoD and global enterprises that often depend on legacy applications that were built decades ago, and are no longer supported by the vendor and/or cannot be easily upgraded.
Hardware vulnerabilities	Modern processor information vulnerabilities such as Spectre, Meltdown, and their many variants allows for code running on the lesser privileged side of a security boundary to read data held on the more privileged side. In less than 6 days from the Spectre and Meltdown initial release, at least 139 variants of malware were appearing in the wild, of which a significant number were based on the JavaScript proof of concept[xix].
Patch cycles	A 30-person cyber security team spends an average of 321 hours per week (equivalent of 8 full time employees) managing vulnerability response and patching. Last year, an average of 40 new vulnerabilities were published per day, and 50% of exploits were published within 14 days[xx]. When patching takes 67 days, there is a clear window for an exploit to breach a network before the vulnerabilities are patched.
False positive volume	With the constant onslaught of attacks, a large volume of security events (4,000+ per day) is generated that a security operations center (SOC) needs to triage. However, at least 2,900 of these are usually false positives. With nearly nine out of ten organizations experiencing a shortage of IT security personnel, it's no surprise 63% of CISOs are concerned about the SOC team alert fatigue[xxi].
Social engineering	The weakest link in any security strategy remains the end user. Using social engineering, phishing continues to have a worldwide impact of $5B, luring people into installing malicious content or disclosing credentials. Last year, 95% of successful phishing attacks were the result of a user being tricked into installing software[xxii].

Key DoD Mission Access Use Cases

The DoD's exposure to attacks is determined by a combination of factors, including user requirements, activities, connectivity, and infrastructure. Naturally, when DoD systems are connected to non-Dept of Defense Information Network (DoDIN) infrastructure, the propensity for compromise increases dramatically. Below, we examine the issues related to Government Furnished Equipment (GFE) On-Premise connections, GFE Off-Premise, and Non GFE-Off-Premise.

GFE On-Premise:

- The highest percentage of active Internet-facing devices sit within the DoD enterprise, with users interacting directly with the Internet from their work terminals.
- There is no domain separation at the endpoint and mission and Internet traffic traverses a single infrastructure fabric, from the host through to the network itself. Both mission and personal Internet traffic is carried over the Intranet, connected to the entirety of the DoD unclassified backplane.
- The air-gapping of mission-related Internet activity from non-mission is currently not supported, as there is typically no abstraction available for the top-level domains or built-in domain-specific abstraction from the DoDIN, with all browsing traffic running within the same Chrome browser. Aside from air-gapped Internet access, challenges include data exfiltration, data migration, credential theft, and host-based OS and application cyber-attacks.

GFE Off-Premise:

- Off-Premise users pose the greatest security risk, as they do not benefit from the layered network security resources while accessing the DoDIN over commercial network connections using a VPN.
- In cases where a user must perform both DoD work and mission-related Internet transactions, the user's device suffers from the same collapsed host OS and application stack, with limited to no abstraction or virtual air-gapping on the device itself, sharing the same USB, network, OS, and app stacks with the untrusted Internet. As a result, the risk of the host being compromised upon connecting to a captive portal is exponentially higher, and once the host is penetrated, despite an encrypted connection via VPN, the adversary can steal credentials, move laterally across the VPN connection, the remote access solution, etc.
- The ability to securely route personal Internet traffic while off-Premise is paramount to the success of the DoD. For maximum efficiency, organizations should consider hypervisor-based abstraction at the host, assuring isolation of personal Internet transactions, abstracted from the running host system.

Non-GFE Off-Premise CUI/FOUO:

- Access to DoD assets from non-GFE access points creates an untenable challenge as the device is neither managed nor owned by the DoD, however users still have access to DoD information and domains. As such, the integrity of such host system is unknown and unmanaged.
- Of primary concern is securing Controlled Unclassified Information in Off-Premise environments.
- Organizations should consider identification of the device accessing DoD materials on the DoD infrastructure as originating from the public Internet. Separating the host environment from the actual access to the interaction with DoDIN can be resolved by leveraging hypervisor abstraction on the endpoint.
- When running the access application in a protected virtual machine, the focus shifts from the integrity of the actual device to the security of the access VM.
- Enforcing access only via a protected VM on the host system, the DoD can control data migration, data exfiltration, data destruction, or lateral movement from the non-GFE host to the DoD network.
- The Internet connection used, although public, becomes a private, measurable, attestable, and secure connection between the VM itself and the backend DoD resources being accessed.

Implementing a Modern Endpoint Security Stack as the Last Line of Defense

The U.S. DoD is taking advantage of an opportunity to upgrade and modernize the endpoint security stack for the future by leveraging the combination of containment (Application Isolation and Containment) and Endpoint Detection and Remediation (EDR) technologies in concert to address the changing threatscape.

Together, these approaches enable the DoD to respond more quickly to attacks: data collected by the containment solution can be passed to the EDR system, giving it real-time threat detection capabilities, based on information gathered from real attacks, without the time delays associated SOC team analysis.

By combining existing HBSS tools with modern approaches such as Application Isolation and Containment and EDR, organizations can reduce the number of agents on endpoints while achieving the highest level of effectiveness against cyber-attacks and reducing operational costs triaging false positives.

The integration of these tools has proven beneficial in multiple instances where the threat analytics provided by Application Isolation and Containment was used to further refine and harden other layered defenses solutions. Due to the fact that each of these approaches looks at the threat landscape in a slightly different way (for instance, time of the attack, pre- or post-incident, the location of the incident, on the host or inside a contained environment, or through restricting lateral movement on the host or in a contained environment), they are able to provide a more holistic view into what is occurring on both individual endpoints as well as across the DoDIN enterprise.

As attacks grow in complexity, precision, and volume, yesterday's approach to threat intelligence is no longer adequate. Investigating targeted attacks in no easy task. The dynamic behavior of the attackers, the greater variety and availability of local and global threat intelligence sources, and the diversity of threat intelligence data formats can make the aggregation and digestion of threat intelligence into security operations tools more challenging than ever before.

A mixed-vendor environment adds to the difficulty of sharing event data and promoting event visibility throughout the organization. However, McAfee provides a unified, collaborative platform with all of the components for operationalizing threat intelligence, including global threat intelligence feeds, local intelligence creation, real-time sharing of threat information across the DoD infrastructure. McAfee Threat Intelligence Exchange (TIE) aggregates and shares file reputation intelligence across the entire security infrastructure – including disparate components. TIE receives threat information from a number of inputs (e.g. Global Threat Intelligence feeds, STIX file imports, endpoints, etc.) including those external to McAfee.

Collecting data from all points in the infrastructure provides information on threats that may be present only in the DoD or customer environment. In turn, file reputation information is instantly shared across the entire ecosystem to all products and solutions connected to McAfee TIE via the McAfee Data Exchange Layer (DxL). Threat data shared over DXL includes file reputations, data classifications, application integrity, and user context data, which is shared with and among products integrated into the DXL fabric. Integrated threat intelligence operationalizes the ingestion, digestion, and management of threat intelligence, enabling you to increase threat detection accuracy, eliminate manual efforts, and stop adversaries from harming the mission. With improved visibility and enhanced insights on malicious activity across the security ecosystem, the DoD and its agencies will be better prepared to identify and preempt targeted attacks today and prevent them in the future.

Application Containment: Bromium Secure Platform

Application Isolation and Containment operates on the premise of a protect-first design – to isolate external threats that bypass layered defenses. By default, all risky activities involving opening files and clicking on web links from untrusted or unknown sources are hardware-isolated in a single-use disposable container.

Bromium is the leading Application Isolation and Containment vendor stopping threats that other solutions often miss. Using hardware-enforced containerization and real-time threat intelligence, Bromium gives organizations the freedom to allow their users to work without restrictions, fosters innovation, and dramatically increases the overall security posture through sharing of threat forensics with other security solutions in the stack, including EDR.

Key features and benefits of Bromium Secure Platform include:

- Hardware-enforced isolation running on the host, leveraging CPU built-in virtualization capabilities
- Operates below the kernel, reducing attack surface down to a single isolated application process
- Behavioral-based introspection to detect malicious activity
- Application Isolation and Containment applies equally to web- and file-based threats
- Malicious threats can't reach the host OS, kernel, registry, credentials, or internal network
- High-fidelity alerts with no active response required; potential threats have already been isolated and contained
- Forensics details of threats with full kill chain analysis
- No impact from false negatives (missed detections), since true threats are still isolated and contained
- Endpoint Sensor Network, search, and quarantine for accelerated network-wide response

The Bromium Secure Platform provides hardware-enforced Application Isolation and Containment by leveraging existing CPU features including Intel VT-x/EPT and/or AMD V/RVI for Windows 7, 8.1, and 10. Bromium has been shipping the Secure Platform solution for more than 5 years, and current capabilities include support for Virtual Desktop Infrastructure (VDI) and thick clients. The Bromium Secure Platform can help DISA and the DoD address the following needs:

- **Securing Legacy Applications:** DISA and the greater DoD depend heavily on legacy applications to support critical enterprise and mission systems. Such legacy systems are costly and time-consuming to upgrade and thus remain in place even when no longer supported by the vendor. Bromium uses a hypervisor, rendering known and unknown vulnerabilities in these legacy applications irrelevant, allowing the DoD to secure legacy systems while they are in use and during migration to newer platforms and applications.
- **Application Isolation and Containment:** Each endpoint is self-defending. Bromium hardware-isolates execution of untrusted documents/files, executables, websites, untrusted coalition partner networks and content, and untrusted collaboration of content. It also supports secure access to VDI and other remote access environments, automatically remediating each isolated attack. With Bromium, malware is contained and cannot access high-valued information, credentials, or networks.
- **Threat Analysis:** Bromium delivers a detailed trace of malicious execution in real time, including a complete forensic analysis of the entire attack payload. There is no need to look across several enterprise sensors to re-aggregate the malware post-breach, or after data has been exfiltrated. The endpoints and network remain fully protected, while Bromium provides real-time actionable threat intelligence to study the attackers' intent, instrumenting defenses to block that attack across the broader enterprise.

- **Threat Knowledge Sharing:** In addition to real-time visibility into attacks, Bromium offers full integration into existing threat systems, SIEMs, Threat Sharing platforms (ex. STIX), Network/Perimeter Compliance and Visibility tools, Systems Management & Orchestration platforms, as well as Network Cybersecurity Analytics, and other solutions with a simple API.

Endpoint Detection and Response: McAfee Active Response

McAfee Active Response (MAR) provides advanced malware hunting and response capabilities through powerful detect and correct tools. MAR cuts through the noise generated from siloed traditional defenses, empowering analysts to quickly uncover threats anywhere in the environment – whether they're actively propagating, lying in wait, or covering their tracks to avoid detection.

The commonly shared perspective is that threat correction ends when a single endpoint is remediated. DoD security teams may be able to detect and clean up an individual infection, but they don't have the visibility or resources to hunt down that infection everywhere it might have spread; the result is frequent re-infections.

By adding MAR malware hunting and response capabilities, DISA and DoD agencies can close the loop of the detect, correct, and protect stages of the threat defense lifecycle. Analysts will have the ability to proactively search the entire organization to detect similar threats, including attacks that are actively propagating or lying hidden, as well as malware that entered the system months ago and then deleted itself. And, because MAR communicates with McAfee's Threat Intelligence Exchange (TIE) as part of a unified threat defense fabric, the moment a new threat or vulnerability is discovered, that knowledge can be applied to inoculate every other endpoint in the environment. MAR provides single-click correction, customizable triggers and reactions and unified workflows to automate security operations across the full threat defense lifecycle: protection, detection, and correction. The result is a continuously evolving threat model that can conduct all of the listed cyber operations including the ability to adapt to new attack strategies much faster, with less effort, and with fewer resources.

Some of the key McAfee Active Response features and benefits include:

- Collectors enable user to find and visualize data from systems, including files, network flows, registry and process mapping
- Triggers allow for continuous monitoring of critical events and alert on a state change
- Reactions provide preconfigured and customizable actions enabling the ability to hunt and kill threats
- Centralized management with ePO provides a single console to manage McAfee security controls
- Integrated security architecture leverages the data exchange layer to streamline communication with other security products

Solving for Key DoD Mission Access Use Cases with Containment + EDR

By combining the capabilities of Bromium Secure Platform and McAfee Active Response, the DoD and other global organizations can take advantage of dramatically improved overall security posture and risk reduction.

Primary Need of the DoD	Technology to Address the Need
Isolation of any untrusted Internet-based activity, including: email attachments, web-links, and downloads	Bromium Application Isolation and Containment
Threat hunting and response	McAfee Active Response
Legacy application protection when patching is no longer an option	Bromium Application Isolation and Containment
Insider threat detection and response	McAfee Active Response
Triage of unknown/zero-day threats for rapid response	McAfee Active Response using ingested Bromium forensics data
Disaggregated Internet: mission/personal access from single device	Bromium Application Isolation and Containment
Threat sharing to improve preparedness and speed to response	McAfee Threat Intelligence Exchange/Open Data Exchange Layer

Maintaining Operational Integrity in a Compromised State

There are frequent situations in which operational integrity of a High-Value Assets (HVA)[xxii] must be protected regardless of the state of the host, which may be compromised, off the network, or non-GFE.

High Value Asset Access Control Use Cases:

- When each endpoint device shares host resources, a compromised host opens the door for malware to move across the device and laterally onto connected infrastructures, where it can steal credentials, and even exfiltrate data while connected via the common browser and host.
- If a device has access to the DoDIN, it has access to DoD High Value Assets. If a keylogger can be installed and credentials stolen, the adversary can then pivot laterally.

- DoD frequently operates a cloud-based remote web browsing where the DoD may not own or control all the components that comprise the complete end-to-end critical infrastructure, including:
  - Host PCs and thin client devices
  - Wide-area network links
  - Internet links
  - Remote browsing servers
  - Data hosting and colocation centers
- Organizations should consider a solution that can virtually air-gap the potentially compromised host from access to the DoD's High Value Assets. By effectively deprivileging the host and giving the protected application the highest privilege on the system, the DoD no longer needs to be wholly concerned with the integrity of the host. The host itself has no direct connection to the High Value Assets, but can still access them through a protected virtual machine. An air-gapped system is implemented – all within the context of the same domain.
- By implementing a hypervisor-based solution that can support remote attestation, boot measurements, user authentication as well as full control over the access session, the integrity of the host itself is no longer critically important, instead, the DoD can focus all efforts on securing their High Value Assets and access to these environments.
- When combined with Internet abstraction, this approach can help the DoD effectively segregate, abstract, and air-gap the High Value Assets from the NIPRNet and the Internet, as well as a potential threat from a determined insider.
- Such a solution would benefit secure remote access over commercial networks, coalition collaboration, CUI requirements, and contractor support.

Bromium Protected Applications

Bromium Protected Applications™ uses virtualization-based security to create hardened, protective enclaves on any host PC or VDI thin client—even one that has already been compromised by malware. These enclaves load in Secure UEFI bootups, ahead of the host operating system. This ensures the confidentiality and integrity of communications, protected from compromised or malicious hosts. Even malicious host administrators cannot access the Protected App™ VM. Furthermore, Protected App attests the endpoint application state to the remote browsing cloud service—verifying the hardware, hypervisor, application, image, configuration, and more.

Each Protected App enclave creates a "secure tunnel" between the host and the remote service, establishing a VPN connection to the datacenter and providing complete application control per connected application VPN. This way, the host and the remote service can still communicate securely, even if the network itself is unsecured or untrusted.

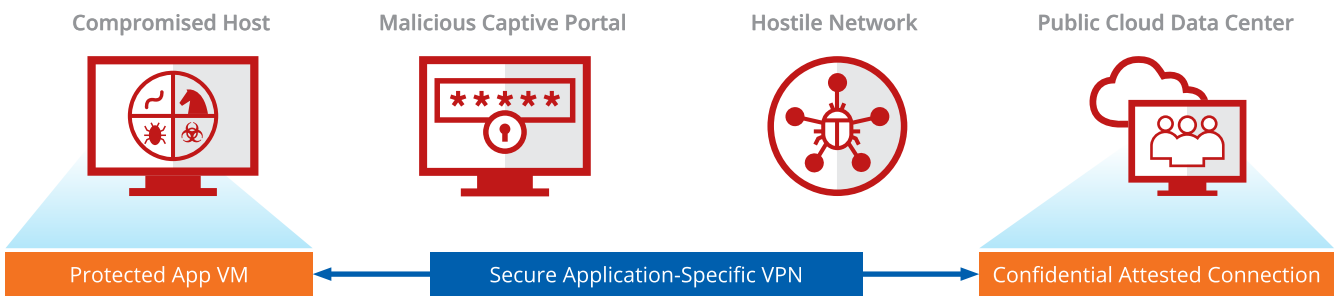

Figure 2: Bromium Protected App protects High Value Assets against compromised hosts

Protected App guards against the following threats for High Value Assets:

- **Keylogging:** Keystrokes users enter while using Bromium Protected App are invisible to the host. Even if a malicious user or malware has compromised the host, the host can't be used to inject keystrokes into the protected VM
- **Memory Tampering:** Because its memory is isolated from the Windows OS, the VM's memory is tamper-proof
- **Disk Tampering:** The VM is isolated and the disk is encrypted, ensuring disks can't be tampered with
- **Kernel Exploits:** Because the VM is independent of the Windows OS, it isn't susceptible to a Windows kernel exploit
- **Prevent Unauthorized User Commands:** Unauthorized commands, including screen captures, downloads, copy and paste, and printing can all be blocked by the solution
- **Man-in-the-middle Attacks.** The solution encrypts all network traffic between the Bromium Protected App client and the secure server. As a result, data can't be viewed in the clear by the user's host OS or when in transit across the network.

Primary Need of the DoD	Technology to Address the Need
High Value Asset protection	Bromium Protected App
Secure remote access to cloud, VDI, hosted applications, etc.	Bromium Protected App
Coalition, third-party, remote worker, or contractor access	Bromium Protected App

Conclusions and Recommendations

This paper covers a lot of ground, proposing novel solutions to address longstanding problems that existing cyber defenses have long failed to meet. Untrusted inbound files from email and the Internet need to be isolated from physical endpoints and networks using virtualization that provides hardware-enforced Application Isolation and Containment separate from the host PC. At the same time, trusted High Value Assets must be protected from compromised clients and networks whenever the end-to-end solution is not entirely controlled by the DoD, using virtualization technology that protects critical assets while guaranteeing user authentication and attestation against interception and abuse.

No single defensive solution will solve every problem, but combining best of breed technologies provides the greatest opportunity for success. When anomalies are discovered, timely and actionable threat information must be shared broadly throughout the DoD in ways that continuously reduce the available attack surface. Bromium's Breachless Threat Intelligence™ from malware attacks in isolation can bolster frontline defenses, while EDR solutions such as McAfee Active Response can quickly identify and eliminate threats across the DoD estate and close off future points of attack.

References:
i G00369430
ii Cybersecurity Ventures 2017 Cybercrime Report
iii https://www.weforum.org/reports/the-global-risks-report-2018
iv https://cdn2.hubspot.net/hubfs/468115/Campaigns/2017-Ponemon-Report/2017-ponemon-report-key-findings.pdf
v https://www.ibm.com/account/reg/us-en/signup?formid=urx-33316&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&cm_mc_uid=52417004412315354854732&cm_mc_sid_50200000=83726071536116250712
vi BBC News: Ransomware cyber-attack threat escalating – Europol
vii ZDNet: Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk
viii The Register: FedEx: TNT NotPetya infection blew a $300m hole in our numbers
ix BTIG cyber security 2018 and beyond
x https://www.verizonenterprise.com/verizon-insights-lab/dbir/
xi https://www.helpnetsecurity.com/2017/09/29/credential-theft/
xii Exploits at the Endpoint: SANS 2016 Threat Landscape Survey
xiii https://www.infosecurity-magazine.com/news/fileless-malware-on-the-rise/
xiv https://arstechnica.com/information-technology/2017/10/equifax-website-hacked-again-this-time-to-redirect-to-fake-flash-update/
xv Bromium sponsored Vanson Bourne research
xvi BTIG cyber security 2018 and beyond
xvii https://www.scmagazine.com/home/news/cybercrime/malware-free-attacks-on-the-rise-as-line-between-cybercrime-and-nation-states-blurs/
xviii https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf
xix https://www.networkworld.com/article/3253898/security/researchers-find-malware-samples-that-exploit-meltdown-and-spectre.html
xx https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf
xxi PBWT: Target's Cyber Insurance
xxii BTIG cyber security 2018 and beyond
xxiii 2 OMB M-17-09 Management of Federal High Value Assets

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all. **www.mcafee.com**

About Bromium

Bromium is the leader in application isolation. We pioneered virtualization-based security to protect your brand, data and people using our patented hardware-enforced containerization with application control, and a distributed Sensor Network to protect across all major threat vectors and attack types. Unlike detection-based techniques, Bromium automatically isolates threats and adapts to new attacks using behavioral analysis, and instantly shares threat intelligence to eliminate the impact. Our technological innovations have earned the company numerous industry awards. Bromium counts a rapidly growing set of Fortune 500 companies and government agencies as customers. **www.bromium.com**

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com