Osterman Research
WHITE PAPER

White Paper by Osterman Research
Published **October 2020**
Sponsored by **Anomali, BIO-key International, MDaemon Technologies and Virsec**

Better Ways to Deal With New Security Threats

Executive Summary

Yesterday's leading-edge security innovations are today's table stakes. As many organizations have ramped up multi-faceted security defenses, threat actors have pivoted to embrace new exploits, new avenues of compromise, and new ways of ensuring a financial payoff from their misdeeds. Criminal or not, adversaries with just as much commitment to wreaking havoc as organizations have to prevent are actively pursuing the next loophole, the next security vulnerability, and the next victim to hold ransom. As security threats change, security defenses need to as well, both reactively to stop current threats, and, more importantly, proactively to get ahead of future security threats.

In this report, we look at the dynamics of the new threat landscape and highlight new security solutions and practices that go beyond the capabilities of conventional solutions.

KEY TAKEAWAYS

- Cybercriminals are not resting on past wins. They are actively seeking new vulnerabilities, new attack vectors, and new ways of both compromising sensitive data and earning a financial payoff. Threat methods are getting more sophisticated and difficult to detect.

- Current cybersecurity threats will remain an issue over the next two years; the emergence of new threats will not diminish the use of phishing, spear-phishing and ransomware, nor attacks directed against misconfigured cloud services.

- Rapid access to new services for productivity and securing time-to-market benefits with cloud services are insufficient decision-making criteria alone; security is a critical aspect. Ditto for hybrid and on-premises infrastructures.

- There are many newer security solutions and practices available to blunt the growing threat arsenal. The reference to "newer" solutions in this report includes solutions that are not necessarily new to the market, but have low adoption and we consider promising.

- New solutions include offerings that move beyond the design principle of threat detection, decrease the attractiveness of targeting a given organization, and offer adaptive security controls, rather than using simple rule-based approaches.

- New (and existing) solutions alone will not win the fight against new security threats; these must be complemented with security best practices.

- The applicability of the threats and solutions in this report to any given organization will depend on multiple factors, including industry vertical and organization size. While not everything in this report will apply to every organization, that determination must be identified positively and revisited periodically.

> ***There are many newer security solutions and practices available to blunt the growing threat arsenal.***

ABOUT THIS WHITE PAPER

This white paper was sponsored by Anomali, BIO-key International, MDaemon Technologies and Virsec; information about each vendor is at the end of this paper.

The Outlook: How Cybersecurity Threats Will Change

In this section, we provide a forecast of how cybersecurity threats will change over the next two years. But first, we briefly touch on threats that will remain.

WHAT REMAINS CONSTANT?

The emergence of new security threats will not result in the wholesale retirement of the current security arsenal. Many current security threats will continue over the next two years, for three primary reasons. First, they work. Current threats have proven effective at gaining credentials, breaching data, and resulting in a financial payoff for cybercriminals. Second, they provide a proven training ground for new cybercriminals entering the market. Third, they are inexpensive to operate at scale—one study found SMEs in the UK were subjected to 65,000 cyberattacks a day, with 4,500 data breaches as a result[i] – all it takes is one employee in an ill-protected organization to take the bait. Threats in the "tried-and-true" category that will continue to have relevance include:

- **Phishing and spear-phishing**
  Broad-based phishing attacks play the volume game for minimal cost to seek out valid account credentials. Spear-phishing uses targeted lures to increase the likelihood of compromising a specific target, despite low message volumes. Data harvested from professional and consumer social networks (often the result of password re-use that makes credential theft easier) matched with data from earlier data breaches enables cybercriminals to build detailed dossiers on targets.

- **Ransomware**
  Despite "do not pay" advice from national cybersecurity advisory groups, paying to get out of a ransomware incident is often faster and less expensive than rebuilding systems, particularly when backup processes are lacking. However, paying in no way guarantees that a bad actor will not release the encrypted data anyway, or will actually provide the encryption keys to enable access to victims' data.

  As firms increasingly hold cybersecurity insurance policies, paying the ransom demands falls on the insurance company concerned. Enterprises, government agencies, educational institutions and healthcare organizations are primary targets for ransomware operators, not least because there is a greater propensity to pay higher ransomware demands than a single, compromised individual could afford.

- **Misconfigured security for cloud services**
  With the proliferation of both sanctioned and unsanctioned cloud services across an organization, the occurrence of misconfigured security settings increases. Amazon Web Services S3 buckets have been a frequent source of data breaches due to inappropriate open levels of security, and customers have also been breached across many other cloud services offering file sync and share. A recent study by McAfee found that organizations have an average of 14 misconfigured IaaS instances running at any time, resulting in over 2,000 incidents per month.[ii]

- **Multi-Factor Authentication (MFA)-Resistant Phishing**
  Cyber criminals have designed phishing attacks that circumvent certain types of multi-factor authentication protections. Carefully created phishing campaigns linking to fake-but-realistic destination login sites have been able to bypass both short message service (SMS)-based and authenticator-app based second factor approaches, enabling successful account credential compromise. Amnesty International noted the use of MFA-resistant phishing attacks on journalists and activists in the Middle East and North Africa. Several security experts have demonstrated similar attack methods.

Paying [ransomware demands] in no way guarantees that a bad actor will not release the encrypted data.

While the above threats will continue, the cybercriminals involved will also step up the sophistication of their attacks over the next several years. We have already seen ransomware transition from data encryption only to data encryption with the threat of publication of exfiltrated data, cybercriminals actively evading security defenses through evasive techniques in malware, and the use of current topics in the media to provide content for phishing campaigns. Many of the latter are sensitive, emotionally charged issues to which people are more likely to respond impulsively, e.g., access to COVID-19 relief funds or hard-to-source protective gear, and the upcoming U.S. Presidential election.

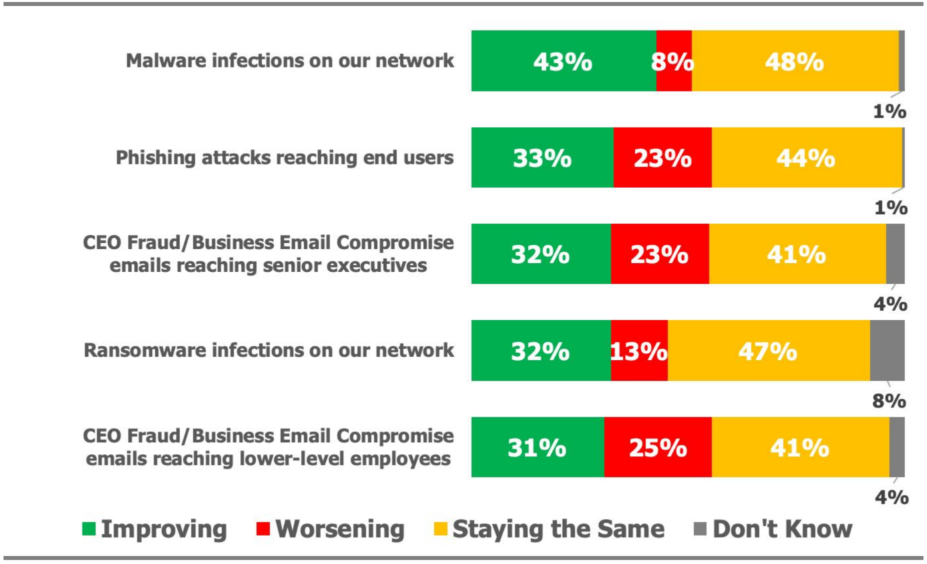
In addition to the above external threats, we do not expect employees, managers and executives to suddenly become security ninjas able to spot a potential vulnerability with their peripheral vision and deal quickly and silently to counteract the attack or threat. People inside the organization will continue to make mistakes (e.g., clicking on a link in an authentic-sounding phishing message), act negligently (e.g., openly publish sensitive data to a website), and in some cases, act in a covert manner to hide their malicious activities. Phishing, ransomware and malware attacks aside, security threats from insiders will remain a leading cause of security incidents, because insiders have so many more direct interactions with sensitive data and applications on a daily basis compared to cybercriminals on the outside.

THINGS ARE NOT GETTING BETTER FOR MOST

Our research found that for most organizations, more conventional threats like malware infections and phishing are not getting better. As shown in Figure 1, 57 percent report that the degree of malware infections is not getting better, while 67 percent report the same about phishing attacks that reach end users. For more difficult-to-detect threats, the situation is even worse.

> ***Cybercriminals are not resting on past wins. They are actively seeking new vulnerabilities, new attack vectors, and new ways of both compromising sensitive data and earning a financial payoff.***

Figure 1
Changes in Various Threats Over the Past Three Years



Source: Osterman Research, Inc.

CHANGES IN FUTURE THREATS

Cybercriminals are not resting on past wins. They are actively seeking new vulnerabilities, new attack vectors, and new ways of both compromising sensitive data and earning a financial payoff. Threat methods are getting more sophisticated and difficult to detect. The next two years are likely to see new and changing threat activity in the following areas:

- **Cloud integration attacks**
  Cloud services have revolutionized enterprise IT infrastructures, but in doing so have created massive, attractive targets for cybercriminals. The prospect of compromising these gigantic data vaults is too good to pass up, and cybercriminals are already seeking out weaknesses in cloud code, piggybacking

on low security authentications, and exploiting widely published but insecure APIs to capture application data. Some forward-thinking cybercriminals playing the long game are even planting vulnerabilities in open source code, to be exploited at an opportune moment against a currently undefined target.

- **Cyber-espionage for hire**
  While cybercriminals will continue to steal trade secrets opportunistically through cyber-espionage, as capabilities to hide their tracks become stronger, less ethical organizations will commission targeted attacks to steal intellectual property and undermine competitors. Payment by Blockchain obfuscates the actual players involved, side-stepping the push for greater transparency in global financial markets, and thus enabling a higher likelihood of non-attribution.

- **Deepfakes**
  Advancements in artificial intelligence (AI) for creating fake images, videos and audio for the purposes of impersonation, fraud and misinformation will increase. Cybercriminals will develop capabilities for turning a target's voice print against them, to enable real-time countermeasures against attempts to verify the veracity of a phishing or business email compromise request. For example, a deepfake of a CEO when combined with a spoofed or hijacked phone number will simplify the approval of fraudulent transactions for cybercriminals.

- **Working from home**
  The COVID-19 pandemic forced the hand of many organizations to suddenly support remote working, and as the effects linger, some organizations are extending remote working approaches. From a cybercriminal's perspective, this is a fabulous trend since it greatly expands the list of places to attack, many of which have fewer cybersecurity protections than traditional office buildings, e.g., consumer-grade home routers, open wireless networks, and fewer device-level protections. It also removes easy face-to-face access to co-workers to check on a suspect email, makes common the practice of receiving audio and video updates from managers and executives (which in the world of deepfakes, can be leveraged to perpetuate authentic-looking scams), and places always-on digital listening devices such as Alexa and Siri in people's workspaces. Unless organizations act decisively to reduce the expanded attack surface with remote working arrangements, cybercriminals will direct future attacks toward these weaker links. And finally, given the mass disruption to employment and future uncertainty over career prospects as a consequence of the COVID health pandemic, some employees are likely to seek greater financial certainty through fraud and other malicious activities against their employer.

> ***Payment by Blockchain obfuscates the actual players involved, side-stepping the push for greater transparency in global financial markets.***

- **Nation-state attacks**
  Nation-state attacks are already a global problem, with Verizon's data breach report in 2019 saying such attacks had almost doubled over the previous year.[iii] Also in 2019, Google detected targeted attacks on over 40,000 Google accounts, with a fifth of accounts receiving multiple warnings.[iv] While the number of successful attacks decreased from the previous year, Google said current attacks showed greater sophistication and intentionality. Nation-state attacks run the gamut from disrupting elections through misinformation campaigns, hindering the operation of critical national infrastructure (e.g., financial markets, energy transmission), influencing government-focused think tanks, and stealing trade secrets. There is also the willingness to play a long game, for example, in building trust with foreign journalists over several years before taking a malicious tack, or compromising the actual target organization through a series of initial compromises at organizations in their supply chain. Nation-state actors rely heavily on spear-phishing attacks and custom exploit kits and invest heavily in evading detection. An increasing number of organizations believe they have been under attack from a nation-state threat group, and this is unlikely to change.

- **Hijacking cloud services**
  Credential theft, security misconfigurations, and code injection attacks offer

several pathways for cybercriminals to hijack an organization's cloud services, either explicitly for a ransom payment of sorts, or covertly for long-term espionage and theft of intellectual property. This threat target becomes ever more attractive, as enterprises move further workloads to the cloud.

- **Tuning AI and machine-learning attacks**
  Already in use by cybercriminals to enable faster creation of zero-day malicious payloads, AI and machine-learning technologies will be further leveraged by cybercriminals. The technology will be used to infiltrate communication channels with messages and responses tightly tuned to the corporate lingo. Other applications will see the technology being used to detect both system vulnerabilities and security defenses in order to design an optimal route for new zero-day attacks against specific targets. Cybercriminals will unleash an escalating game of "who has the best AI" to overwhelm security defenses, and given the removal of human intervention from such attacks, raises the prospect of chaotic and unprecedented effects.

- **AI poisoning**
  AI models only work as well as the training data they've been fed, with facial recognition weaknesses due to racial bias a recent example of poor design. Seeking public data for creating training sets poisoned Microsoft's Tay bot in 2016, but given its open public persona was easy for Microsoft to identify and disable. We expect cybercriminals to attempt poisoning of less public-facing AI models through malicious data sets from compromised public sources, or internal sources by using new persistent footholds in a compromised network. The intent is to have the ability to bypass the AI model under certain conditions known only to the cybercriminals.

AI and machine-learning technologies will be further leveraged by cybercriminals.

- **Vigilant regulators and vigilante consumers**
  New style data protection regulations such as European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have swept the globe, creating vigilant regulators with extensive powers and vigilante consumers who are attuned to the misuse of their data. This new regulatory context demands heightened due diligence when acquiring another company, since culpability for undetected data breaches increasingly sits with the acquirer, e.g., the proposed £99.2 million fine against Marriott International for the data breach at Starwood Group which only came to light after Marriott had acquired the company. Consumers, for their part, empowered by these new regulations, are reporting actual or potential data protection lapses with increased frequency. Getting data protection wrong—or even just less than ideal—is becoming a costly mistake.

- **Beyond email, files and application data**
  Annoying an organization through a ransomware attack against servers and devices is financially painful, but crippling, undermining, or chaotically influencing operational technology is life-threatening. As connected software spreads into new spheres of life—the buildings people work in, the cars they drive to and from work, and even entire cities themselves—new vectors for compromising are made available to cybercriminals. Weaponizing buildings, cars and cities is a growing threat of concern, for example, in compromising traffic light routing instructions to cause accidents, or infiltrating the controls of a smart building to imprison its inhabitants and change airflow dynamics and chemical composition.

The Challenge: Productivity Plus Security

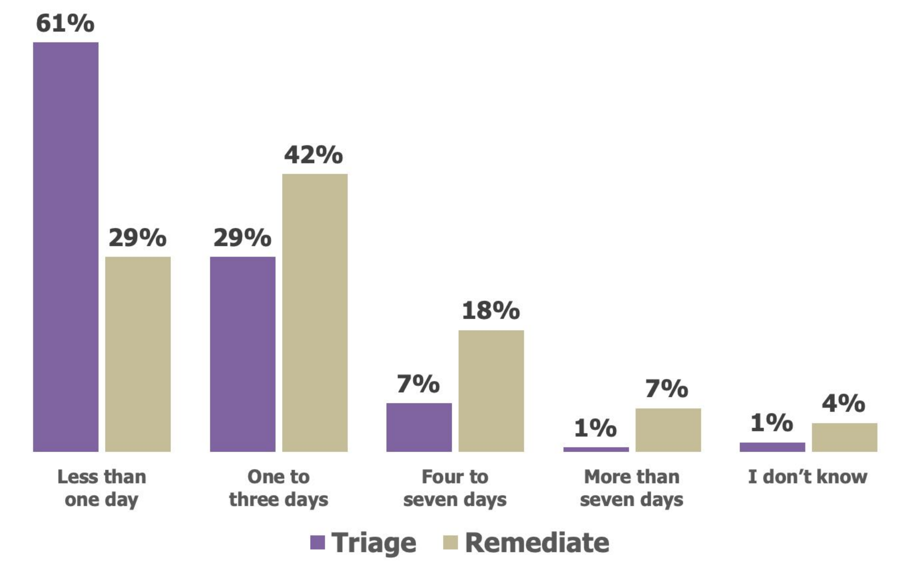
In the face of a growing threat arsenal, organizations need to re-think the balance between productivity and security. The headlong dash to new cloud services offers rapid access to new services for productivity, securing time-to-market benefits as opposed to building on-premises infrastructure. But productivity and speed in moving to the cloud are insufficient decision-criteria; security considerations are a critical aspect. Neither organizations with hybrid infrastructures or those that have stayed away from cloud services and have on-premises infrastructure only are exempt from security considerations.

FIXING PROBLEMS TAKES TIME

One of the problems that security analysts and other security staffers face is the length of time required to address threats and then remediate them. As shown in Figure 2, only about three in five organizations can triage an internal threat in less than one day, and fewer than one-third can remediate such a threat in less than a day. What this indicates is that security teams are not detecting, identifying and resolving threats nearly as quickly as they would like, indicating that new ways of doing things are required.

Only about three in five organizations can triage an internal threat in less than one day.

Figure 2
Length of Time to Triage and Remediate Internal Threats



Source: Osterman Research, Inc.

SECURITY FROM THE BEGINNING

Cultivating a security-from-the-beginning approach involves three essential steps:

- **Update**
  Update your security assessment for current and planned cloud and on-premises infrastructure, along with up-to-date analysis of the security threats and incidents happening at your organization. Match your security assessment against current IT security approaches designed to prevent, mitigate, and rectify threats. Highlight weaknesses and areas of concern in light of the changing threat context. Having an up-to-date data security assessment is the foundational analysis required for making effective plans, a situation that too few organizations have taken.[v]

- **Evaluate**
  Evaluate new security solutions and services to address the weaknesses and areas of concern identified in Step 1. This is also the place to re-evaluate the number and diversity of cloud services currently in use, and consider if fewer but better cloud services through a vendor consolidation program of work would

both reduce the attack surface and increase productivity through simplified workflow approaches.

- **Embrace**
  Embrace up-to-date best practices for security. Some recommendations from earlier years are no longer current, and various new best practices have become of high priority.

POOR SECURITY = POOR PRODUCTIVITY

Ultimately, discounting security considerations undermines business productivity. Three major negative effects are commonly felt when security is compromised:

- **Brand and Reputational Damage**
  Data breaches, ransomware attacks and other cybersecurity incidents raise doubts in the minds of customers (and business partners) as to the trustworthiness of the organization involved. In the UK, 44% of adults said they would semi-permanently stop using an online company if a data breach was uncovered.[vi] In the educational space, 65% of students are less likely to apply to study at an institution with a poor history with data security.[vii] It's unclear yet what reputational cost the SANS Institute will bear for the breach of data on 28,000 customers this year after a successful phishing attack, but as a provider of information security training, certification, and research, it's embarrassing.[viii]

- **Financial Penalties**
  The GDPR has drastically raised the financial penalties possible for data security lapses, using the annual revenue of the organization as the reference point in assessing punitive damages. The proposed fine against Marriott International of £99.2 million has already been mentioned, due to the compromise of data on over 300 million guests. In comparison, the Equifax data breach of about half that number of people only resulted in a £500,000 fine since it fell outside of the GDPR timeline and hence wasn't revenue linked.

- **Financial Outlay for Incident Response and Rectification**
  Organizations bear a high cost to rectify incidents and systematic weaknesses in their security processes and systems after an incident and have the heat of the public spotlight to contend with as well. As a consequence of a spreadsheet containing personal information being exposed online for 40 minutes in late 2019, the UK government department responsible instituted a data protection program with a budget of up to £2.25 million.[ix] Firms have had to cease operations temporarily due to the clean-up required after a ransomware incident, and some smaller firms have decided to close up shop entirely rather than try to recover.

> ***Ultimately, discounting security considerations undermines business productivity.***

Solutions and Services

Our research found that there are some significant differences between what IT and security departments have deployed to protect against cybersecurity threats and what security-focused decision makers and influencers would like deployed in their infrastructure. As shown in Figure 3:

- The leading solutions that security teams wish they had versus what they currently have deployed (as noted in the "Difference" column) are memory attack detection; cloud-based EDR, SIEM and SOAR; a cloud-based threat intelligence platform; and threat intelligence feeds and blocklists.

- The leading solutions that security teams would like to have in their infrastructure (as noted in the "Preferred" column) are anti-virus and anti-malware on endpoints; cloud-based secure email gateways and secure web gateways; and threat intelligence feeds and blocklists.

Figure 3
Currently Deployed and Preferred Security Solutions

Solution	Preferred	Deployed	Difference
Anti-virus or anti-malware solution on endpoints	63%	86%	-23%
Cloud-based secure email gateway	58%	59%	-1%
Cloud-based secure web gateway	54%	38%	16%
Threat intelligence feeds/blocklists	54%	35%	19%
Office/Microsoft 365 Advanced Threat Protection	51%	41%	10%
Cloud-based threat intelligence platform	47%	26%	21%
Office/Microsoft 365 Exchange Online Protection	45%	49%	-4%
Cloud-based EDR solution	44%	20%	24%
Web application firewall (WAF)	43%	54%	-11%
Server/host protection solutions	43%	45%	-2%
Cloud-based SIEM	43%	20%	23%
Cloud-based DLP	42%	26%	16%
Host-based intrusion protection system	41%	48%	-7%
Web application security solutions	40%	43%	-3%
Memory attack detection	40%	15%	25%
On-premises secure web gateway	38%	56%	-18%
On-premises secure email gateway	36%	55%	-19%
Host-based runtime application self-protection	35%	23%	12%
On-premises DLP	33%	34%	-1%
On-premises SIEM	33%	33%	0%
Cloud Application Security Broker	31%	12%	19%
Cloud-based SOAR	30%	7%	23%
On-premises threat intelligence platform	29%	29%	0%
On-premises EDR solution	27%	23%	4%
On-premises SOAR	22%	10%	12%

Source: Osterman Research, Inc.

There are many newer security solutions available to blunt the new threat arsenal.

There are many newer security solutions available to blunt the new threat arsenal. In this section, we look at new solutions in four categories, and we use the term "new" to refer to both chronologically newer offerings, as well as solutions that are not new to market but have low adoption despite their promise. Some of these solutions are offered as new products to deploy on-premises or subscribe to in the cloud, and some are being incorporated into broader security offerings. The four categories are:

- Solutions that move beyond a detection mentality, seeking to move beyond a reactive stance to the latest cybercriminal attack.

- Solutions that decrease the attractiveness of targeting a given organization, by increasing the cost and complexity of making an attack work.

- Solutions that move beyond simple rule-based security enforcement, opting instead for adaptive security controls that take the wider context of the proposed action into account.

- Solutions that don't fit into the three categories above. The "other" category.

SOLUTIONS THAT MOVE BEYOND DETECTION

Detecting threats before they inflict havoc has been a key design point for many security solutions. Signature-based methods worked on matching previously catalogued threats with current happenings. Advanced threat protection services have looked at the behaviors of messages and files in an effort to detect new, zero-day threats. The assumption is that which can be detected can then be mitigated, neutralized or sanitized. As threats have become more sophisticated, while detection-based approaches are not without ongoing merit, various new security solutions take a more proactive stance in threat neutralization. We look at four beyond detection solutions in this section.

CONTENT DISARM AND RECONSTRUCTION

Instead of playing a game of escalation where security solutions embrace ever-advancing methods of detecting threats in documents and files as cybercriminals embrace ever-advancing methods of evading detection and introducing new threats, Content Disarm and Reconstruction (CDR) services strictly enforce a normalization process that just removes anything from a document or file that could be leveraged maliciously. The core assumption is that all active content is suspicious, and even for perfectly clean documents and files, the technology proactively removes even the possibility of malicious activity. CDR works by breaking each newly received document into its various discrete components, stripping out the components with active content that could be malicious, and then recompiling the document in a sanitized form. Macros, URLs, and embedded code, among others, are neutered. The recipient of the document gains a well-formed document ready to run, but without the threat vectors inside.

> ***Detecting threats before they inflict havoc has been a key design point for many security solutions.***

WEB ISOLATION

In principle, what CDR does for newly received documents, Web isolation does for all activity in a Web browser, in that it forces a normalization of activity to remove threats. While a user interacts with web pages, sites and cloud services through their browser as they normally would, what's actually happening in the background is that all activity is executed in a remote virtual environment rather than on a corporate device connected to the corporate network. The remote activity is displayed in the user's web browser, but no web content directly interacts with the user's device. Web isolation technology therefore prevents zero-day exploits, ransomware attacks, malvertising, and credential phishing exploits. If the web content is malicious, the remote virtual environment is terminated without having an effect on the user's device. Web isolation technology does not have widespread usage, despite its promise for significantly reducing successful attacks, and despite being around for some time already.

APPLICATION MEMORY FIREWALL

An application memory firewall prevents deviations in how memory is used by an application. Each application has a normative profile of expected behavior—which can be mapped by analyzing its baseline conventions and instruction sets—which means that unexpected behavior that falls outside of the normative profile is suspect and potentially malicious. When such behaviors are identified by the application memory firewall, it can take action automatically to prevent the continued execution of the abnormal instruction. Application memory firewalls protect against fileless attacks, memory corruption attacks, and buffer overflow attacks, among others.

SymTCP FOR PROACTIVE ANALYSIS OF VULNERABILITIES

Deep packet inspection (DPI) aims to detect malicious payloads or threat-laden components in network traffic. The problem is that DPI services often use a simplified version of the transmission control protocol (TCP) stack in comparison to the server it is seeking to protect. If an attacker can identify the differences between the simplified TCP stack and the full stack being used by an organization, they can create specially crafted malicious packets that trigger the DPI to mark the traffic as clean, which is then passed through. Developed by the United States Army and the University of California, and released as an open source project, SymTCP is a new method to programmatically identify the differences between a DPI's implementation of TCP and the full stack implementation on other servers. Once differences are identified, it provides directions for developers to resolve TCP implementation weaknesses in their DPI service, or for organizations to strengthen security defenses against such weaknesses.

PREDICTIVE ATTACK ANALYSIS

The use of predictive attack analysis using the MITRE ATT&CK framework can be useful in profiling adversaries, campaigns, vulnerabilities and TTPs in order to identify already known and common attack techniques and vectors. Moreover, this approach can enable monitoring of networks and hosts for precursors to attacks so that cyber-attacks can be anticipated and addressed before they actually hit.

The use of predictive attack analysis can also be useful in addressing fast flux networks, a technique used by a number of botnets to obfuscate the domains they use for phishing websites, those used to distribute malware, and so forth. A fast flux network associates multiple IP addresses with a single domain name and then rotates through them frequently to make them more difficult to detect. For example, the Avalanche botnet has used in excess of 800,000 malicious domains since its inception, and these domains can have their IP addresses changed as frequently as every five minutes. One technique in analyzing and defeating fast flux botnets is by predicting the domains that will be generated through the use of domain-generation algorithms (DGAs). DGAs are normally used to generate command-and-control domains that are then employed to communicate with infected machines in a botnet. Reverse engineering DGAs can be used to predict domain names that will be employed by bad actors and then populating DNS blacklists with these domains, but the process can be defeated. Alternatively, some vendors enable the interception of DNS queries and then enable predictive capabilities to determine if a particular domain was generated by a DGA or a human.

The use of predictive attack analysis using the MITRE ATT&CK framework can be useful.

SOLUTIONS THAT DECREASE ATTRACTIVENESS OF TARGETS

Low cost for high payoff is an attractive proposition for businesses entering a new market. Cybercriminals think the same way. The following solutions seek to decrease the attractiveness of targeting a given organization, by increasing the difficulty of landing a successful attack.

VIRTUAL DISPERSIVE NETWORKING

Traditional networking approaches establish secure point-to-point connections for routing data to its destination, but if the connection is compromised, so is the totality of the data conveyed over it. Virtual dispersive networking divides data into many smaller units, routing each over disparate network paths using diverse networking protocols. The technology draws inspiration from wireless radio designs used in military scenarios, and offers increased speed of transmission, improved network resilience, and better data security. If a hacker was to intercept one of the network paths, they would only gain the portion of the encrypted data routed accordingly.

PASSWORDLESS AUTHENTICATION

Compromised user credentials are responsible for a very high proportion of security breaches; if a phishing attack can gain someone's username and password, it's easy to get into corporate data repositories. Passwordless authentication is based on the principle that reliance on the idea of passwords themselves is the problem, and a completely new way of enabling stronger authentication is needed. Physical hardware tokens are one way of enabling passwordless authentication; the token uses public key cryptography to provide secure access for a given user to an application or service, and without the physical token, access is not granted. Hence the attractiveness of deploying phishing campaigns for user credentials is greatly reduced, since there are no user credentials to compromise. Access to the physical hardware token is needed for system access, but if the token is biometrically linked with a given user as well (e.g., fingerprint scan), even possession alone is insufficient.

DECEPTION TECHNOLOGY

Creating fake but realistic systems, credentials and files that indicate a potential payoff for a hacker offers a method of redirecting hacking activity away from production systems into decoy ones, and providing early detection of malicious activity to security staff. Deception technology creates authentic-looking systems, credentials or files that are actually traps. Any activity in, around or with these traps raises alerts for the security team, and captures a profile of the hacker's behavior which can be used to strengthen defenses. Falling for a trap means the hacker wastes their time and effort while also providing a free masterclass on how they work and operate.

SOLUTIONS THAT LEVERAGE ADAPTIVE SECURITY CONTROLS

Simplistic methods of security fail in the dynamic world in which we live. The current and coming threat landscape requires approaches that take into account a greater number of variables. In this section, we look at solutions that enable adaptive security controls.

ZERO-TRUST APPROACHES

The principle of zero trust is that no user or device is trusted by default; all are potential threats until proven otherwise. Based on an assessment across an assortment of relevant criteria—such as the user identity, the type and state of the device, the network from which the user is connecting, the compliance of the endpoint with the organization's baseline security profile—access to a given network or cloud resource is either given in full, offered in a limited form, or denied. Requesting access to further networks or resources forces the recalibration of these criteria, so that every user request is assessed for its validity and security soundness. For example, an executive requesting access to a cloud system from the corporate network using a corporately controlled device will be given a different access experience than when they connect from an open Wi-Fi network at a hotel in a foreign country from their personal tablet.

> ***Deception technology creates authentic-looking systems, credentials or files that are actually traps.***

CONTEXT-AWARE BEHAVIORAL ANALYTICS

With insiders being a significant cause of data breaches and inappropriate system access, context-aware behavioral analytics provides ongoing analysis of the totality of each user's interactions with devices, systems, networks and cloud resources. It uses AI and machine learning to create a picture of normal behavior, so that abnormal deviations can be highlighted and investigated for potential fraud, security vulnerabilities, malware execution, or other red flags. The behavior of people performing similar job roles can be cross-analyzed to quickly create a relevant baseline for each employee, and to highlight potential areas of concern, such as connecting to corporate resources after midnight when no-one else is doing so. Normalized behavioral patterns can also be leveraged for automating heightened security demands—such as a new multi-factor authentication request—when something out of the ordinary is detected. Context-aware behavioral analytics is a rapidly maturing technology, but lacks widespread adoption.

DEVICE-BASED AUTHENTICATION

As a further safeguard against the use of compromised user accounts to gain access to corporate network and cloud resources, device-based authentication limits the possibility of access to known and trusted devices only. Even if a hacker has valid credentials, their use of an unknown device with those credentials is flagged as invalid and thus blocked—along with a notification of a potential credential breach. Restricting access to corporately approved, known devices that meet current minimum-security standards for encryption (among other indicators), limits the attack surface significantly. For further protections, hardware-based authentication can be built into the device rather than relying on an external hardware token, and/or devices are explicitly linked with specific user accounts so that any user can only login with the devices that have been attributed to their user account. Such approaches cut off the security threat of using any user account with any device for access.

DIVERSIFYING THREAT INTELLIGENCE SOURCES

One approach to fending off threats is to go it alone and perform all the analysis based on the data points you see within your organization. It's a costly approach, however, since you have to suffer through all of the associated breaches and security incidents. A better and less costly approach is to gain a wider viewpoint on current threats and threat trends by accessing threat intelligence derived from the analysis of threats across a much higher number of organizations. Threat intelligence services provide early warning of newly identified threats that might not have hit an organization yet, and newer services combine the automated deployment of protections against such threats without human intervention. Newer threat intelligence services also trawl through historical security logs to discover whether new threat intelligence can pinpoint previous evidence of undetected incidents or breaches.

> ***Threat intelligence services provide early warning of newly identified threats that might not have hit an organization yet.***

OTHER SOLUTIONS AND SERVICES

There are a variety of other solutions focused on dealing with current and future threats:

- **Data loss prevention (DLP)**
  DLP offers automated protections against inappropriate and unauthorized sharing of sensitive, confidential or protected corporate data. It relies on classification of data sources and documents containing types of data that need elevated protection, and for both email traffic and file sharing activity, offers a way of preventing the majority of unintentional data leaks. In some scenarios, it can also prevent data exfiltration as a consequence of an advanced persistent threat wrapping up and sending out sensitive data. As more end user applications gain capabilities for automated data classification, this added context can be taken into consideration by next-generation DLP solutions.

- **Domain-monitoring services**
  The proliferation of new global top-level domains has enabled unauthorized actors to register new extensions for well-known brand names, thereby offering the ability to masquerade malicious email traffic as authentic, or create copycat websites that present as the real thing while hiding exploits, malicious forms, or compromised downloads. Domain monitoring services track the creation of new domains using corporate brand names, for both early detection of new vectors of impersonation and initiating action to stop cybersquatting activity. In some industries, it is a massive problem; a recent study by ImmuniWeb in the financial services industry discovered 6,500 cybersquatted domains that had an illicit, fraudulent or potentially deceptive nature.[x]

Best Practices and Next Steps

New (and existing) security solutions alone will not win the fight against new security threats; these must be complemented with security best practices. In this section, we look at several best practices that organizations should implement to protect their users, critical data assets, and finances.

DO THE BASIC THINGS RIGHT

The advanced security solutions we've profiled in this report will fall short of their promise if basic security protections are missing or insufficient. In other words, embrace the newer solutions without giving up on doing the basic things right. These include having as few authentication systems as possible (one is ideal), controlling access rights and expiring user accounts as soon as possible, effective user training and guidance, clear change communications, background checks on new employees to limit the risk of infiltration by a malicious actor, no use of administrator-level user accounts for non-administration daily work**,** and patching servers, applications, routers and endpoints as soon as possible. Maintaining an up-to-date enterprise security and risk register should also be a core aspect of doing the basic things.

EMBRACE SECURITY-BY-DESIGN

Security as a primary design construct is an essential mindset and approach in order to steer clear of current and coming security threats. Security considerations as a bolt-on once services and new APIs have been developed doesn't work; applications must be built securely from the beginning. It must also be a primary consideration when evaluating the suitability of new cloud service providers, along with how duties are segregated and rotated for IT and security administrators.

MINIMIZE THE ATTACK SURFACE

Be proactive about removing potential footholds where cybercriminals could start. For example, keep systems patched against known vulnerabilities, use conditional access policies to reduce the ability for credentials alone to be used for system access, and harden email systems against spoofing and impersonation through strong email authentication approaches. Use network isolation and segregation approaches to decrease the ability for a single compromised device to spread malicious payloads. Set policies on accessing personal social media accounts on government networks (because malicious links can be shared without going through a secure email gateway), and limit access to government systems from home or unmanaged devices.

> ***Be proactive about removing potential footholds where cybercriminals could start.***

ASSIGN RESPONSIBILITY

While every employee (and manager and executive) has a personal responsibility for good security practices in their work, a specific individual must hold the ultimate responsibility and unified leadership for security across the organization. This includes the leadership authority and responsibility for the enterprise-wide security and risk assessment, scoping high-level initiatives to strengthen security defenses, and coordinating with the various security teams responsible for infrastructure, cloud services, user training, and incident response.

REDUCE THE DATA BREACH FOOTPRINT

Don't hang on to data and documents that have no ongoing value. For data subject to retention requirements, use strong encryption or pseudonymization approaches to obfuscate the data and increase the difficulty of breaching clear text data sources. Alternatively, migrate such data from production systems to an archival repository with tighter access security controls. For data that can be deleted or erased, get rid of it as soon as possible. There are policy-based ways of classifying data and ensuring automatic deletion of stale data.

REDUCE THE DATA BREACH HANDHOLDS

The same best practice applies to user accounts. Create a joined up offboarding process so that when a user leaves the organization due to employee cessation or termination, their user account that provides access to network, cloud and system resources is immediately deactivated. This immediately closes off the ability for an attacker to compromise a valid but unused user account through a brute force attack, thereby gaining access to whatever network, cloud and system resources the individual held during the course of their employment. The same approach should apply to contractors, temporary workers, and people with guest user access.

HARDEN PROCESSES FOR COMMON ATTACK VECTORS

Business email compromise attacks frequently seek quick monetary gain through fraudulent invoicing scams or by redirecting valid payments to a recently revised bank account number, the latter of which does happen but is not a common occurrence for any given payee. Strengthen the checks and balances on initial invoicing requests and how employees and suppliers can revise their bank account number, such as through additional out-of-band verification or two-factor authentication mechanisms set up in advance. Move away from email-only requests being sufficient to change a bank account number.

STRENGTHEN IDENTITY ACCESS CONTROLS

Strong, complex, frequently changed, and unique passwords are not working. Users forget them, incrementally numerate passwords to simplifying recall, or write them down. Once credentials have been compromised – even if it's a long password or passphrase – cyber criminals still have access. Strengthen access controls through new approaches that don't rely on passwords, either by removing passwords altogether in favor of FIDO2-enabled passwordless authentication or other modern authentication mechanisms.

Biometric authentication should seriously be considered because it provides the dual benefits of users not have to remember their login credentials, and it enables roving users to authenticate without a token. While tokens are a useful means of authentication and provide a more secure experience than the use of login credentials, they still enable sharing of devices. Biometrics enables a strong identity access solution.

EMPLOY AN INTELLIGENCE-DRIVEN SECURITY OPERATION

The growing complexity and sophistication of cyberattacks underscores the need for organizations to become more proactive in their approach to security instead of detecting and remediating threats after they have occurred. For example, AV-TEST reports that annual detections of new malware samples have been increasing steadily year-on-year, from 470 million in May 2015 to 903 million in May 2019. Moreover, one-half of malware samples in 2019 were zero-day threats[xi]. Consequently, there is a critical need for a proactive, threat intelligence-driven approach to cybersecurity that will enable security teams to anticipate threats and protect against them before they occur. The key to this proactive approach to security is the use of big data analysis that will enable the scaling of threat intelligence to enable real-time visibility into external threats.

> ***Biometrics enables a strong identity access solution.***

Conclusion

We have taken a broad spectrum look at the evolving threat space in this report, and considered new security solutions and approaches that can be used to address these. The applicability of these threats and solutions to any organization will, however, depend on multiple factors including industry vertical, organization size, and the types of data held and processed by the organization. Not everything in this report will apply to every organization, but that determination must be identified positively and revisited periodically.

Sponsors of This White Paper

ANOMALI

Anomali® delivers intelligence-driven cybersecurity solutions, these include Anomali ThreatStream®, Anomali Match™, and Anomali Lens™. Private enterprises and public organizations use Anomali to gain unlimited visibility, speed time to detection, and constantly improve security operations. Anomali customers include more than 1,500 global organizations, many of the Global 2000 and Fortune 500, and large government and defense organizations around the world. Founded in 2013, it is backed by leading venture firms including GV, Paladin Capital Group, Institutional Venture Partners, and General Catalyst. Learn more at www.anomali.com

www.anomali.com

@Anomali

general@anomali.com

+1 844 484 7328

BIO-KEY INTERNATIONAL

BIO-key is a pioneer and innovator in one, we are recognized as a leading developer BIO-key International is an innovative provider of access management & biometric identity solutions that provide convenient and secure access to devices, information, applications, and high-value transactions. BIO-key offers the simplicity and flexibility required to secure the modern digital experience for all users. Backed by decades of expertise, BIO-key has a proven track record of successful Identity & Access Management (IAM) project delivery and strong customer relationships.

BIO-key PortalGuard is the only complete access management platform with industry leading biometric identity options for single sign-on, multi-factor and adaptive authentication, and self-service password reset. PortalGuard supports all deployments, whether cloud, hybrid, on-premise or as a customized enterprise solution.

As a leading developer of biometric identity solutions, BIO-key turns a fingerprint into an authentication method. BIO-key WEB-key is a comprehensive, multi-tenant, enterprise biometric identity platform built around one of the world's most accurate and scalable biometric engines, offering more power than any low-level SDK. With privacy and compliance features, WEB-key is designed to provide a highly configurable biometric experience as an integrated component of any Identity and Access Management (IAM) strategy.

WEB-key works seamlessly with the BIO-key line of high-quality, low-cost Microsoft-qualified Windows Hello USB scanners as well as over 30 fingerprint readers from most major manufacturers. With BIO-key there's no need to remember passwords, combination or carry a key, BIO-key sells convenience.

www.bio-key.com

www.linkedin.com/company/bio-key-international

info@bio-key.com

+1 732 359 1100

MDAEMON TECHNOLOGIES

MDaemon Technologies is a recognized pioneer and industry expert in email server and email security gateway software that is trusted by organizations in over 140 countries. For more than 20 years, our mission has been to help companies maintain secure email communication by delivering reliable, affordable software and services that require minimal effort to manage and maintain. Our products, the MDaemon Email Server is a leading alternative to Microsoft Exchange and 365. The MDaemon Security Gateway is a trusted email gateway solution that protects Microsoft Exchange, 365 and other email servers. Industries as diverse as healthcare, government, finance, education, manufacturing and transportation use our products because they offer administrative control and flexibility combined with strong security and reliability. We offer a variety of deployment options including virtual, cloud, or on-premise environments. Companies can purchase our products directly via our website, or through a global network of resellers and MSPs. For more information, visit www.mdaemon.com.

www.mdaemon.com

@MDaemon_Email

info@mdaemon.com

+1 866 601 2586

VIRSEC

Security technology has not kept pace with the rapid shift to virtual infrastructure, and disappearing network boundaries, and advanced hackers are easily exploiting application weaknesses with fileless and memory-based attacks.

At Virsec, we believe that a new approach is required to counter today's threats. Instead of relying on signatures of past attacks to guess what's coming next, Virsec precisely pinpoints threats at the source, within business-critical applications. Our platform maps correct application behavior, and instantly detects and blocks deviations caused by attacks. This deterministic approach stops threats in real-time, delivering unprecedented accuracy, without false positives. Virsec protects any application, patched or unpatched, across the full application stack from web threats to binary memory-based attacks.

virsec

www.virsec.com
@virsecsystems
info@virsec.com
+1 877 213 3558

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

[i] Robert Walters and Vacancysoft, Technology Sector Report July 2020—Cyber Security, July 2020, at https://vacancysoft.com/technology-sector-report-july-2020-cyber-security/

[ii] McAfee, Cloud Adoption and Risk Report 2019, November 2018, at https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-cloud-adoption-risk.pdf

[iii] Craig Hinkley, Nation-State Cyberattacks: It's Bigger Than Iran, February 2020, at https://gcn.com/articles/2020/02/03/nation-state-attacks.aspx

[iv] Davey Winder, Google Confirms 40,000 Nation-State Cyber Attack Warnings Issude, March 2020, at https://www.forbes.com/sites/daveywinder/2020/03/27/hacker-threat-google-confirms-40000-nation-state-cyber-attack-warnings-issued/

[v] NetSec, 47% of UK IT Leaders Say Security Strategies Have Not Been Updated to Account for Their Cloud Environments, August 2020, at https://www.netsec.news/47-of-uk-it-leaders-say-security-strategies-have-not-been-updated-to-account-for-their-cloud-environments/

[vi] Catherine Wycherley, 4,500 Successful Daily Cyber Attacks on UK SMEs, August 2020, at https://gdpr.report/news/2020/08/21/4500-successful-daily-cyber-attacks-on-uk-smes/

[vii] Redscan, The State of Cyber Security Across UK Universities, July 2020, at https://www.redscan.com/news/state-of-cybersecurity-uk-universities-foi-report/

[viii] Bradley Barth, SANS Institute Breach Proves Anyone Can Fall Victim to a 'Consent Phishing' Scam, August 2020, at https://www.scmagazine.com/home/security-news/data-breach/sans-institute-breach-proves-anyone-can-fall-victim-to-a-consent-phishing-scam/

[ix] Gov.uk, Cabinet Office Personal Data Delivery Enhancement, GOV.UK Digital Marketplace, August 2020, at https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/12778

[x] ImmuniWeb, State of Application Security at S&P Global World's 100 Largest Banks, July 2019, at https://www.immuniweb.com/blog/SP-100-banks-application-security.html

[xi] https://www.cynet.com/blog/half-of-the-malware-detected-in-2019-was-classified-as-zero-day-threats-making-it-the-most-common-malware-to-date/