vmware® Carbon Black

2020 Cybersecurity Outlook Report

In the search for clarity in the modern attacker vs. defender battle, it's all about behaviors

Rick McElroy
VMware Carbon Black Security Strategist

Greg Foss
VMware Carbon Black Senior Threat Researcher

Andrew Costis
VMware Carbon Black Threat Researcher

A VMware Carbon Black Threat Analysis Unit (TAU) Publication

Table of Contents

Executive Summary

The conflict of “good vs. evil” is a theme that’s captivated humanity throughout history, spanning religion, ethics, philosophy, politics, art, literature, and cinema. Often with larger-than-life characters leading the narrative, the “good vs. evil” conflict reveals humanity’s intrinsic desire to be safe amidst an omniscient and, often, ephemeral sense of fear.

In cybersecurity, this conflict plays out on a daily basis, where “good” is represented by the unsung cybersecurity heroes and “evil” is represented by an aggregation of nation-state actors, cybercriminals, hackers, industrial spies, hacktivists, and cyber terrorists - all with different agendas rooted in a desire to tip the balance of power in their favor.

In order to shift this balance of power, certain behaviors are required. We’ve often said that understanding cybersecurity comes down to understanding attacker behaviors. In this report, we use key data from cyberattacks seen over the last year to tell a clear story on how attackers are evolving and what defenders are (and should be) doing to evolve their own behaviors.

Using the MITRE ATT&CK™ framework as the backdrop for our research, this report uncovers the top attack tactics, techniques, and procedures (TTPs) seen over the last year and provides specific guidance on ransomware, commodity malware, wipers, access mining, and destructive attacks.

Of note, our data set has been expanded for this annual report. Included in our analysis this year is attack data from across the VMware Carbon Black Cloud, publicly available sources, and the dark web.

We’ve also invested heavily in expanding our scope for “behaviors” this year. In addition to focusing on attacker behaviors, we’ve commissioned a study from Forrester Consulting to determine the specific behaviors exhibited by defenders - namely the CISOs and CIOs charged with holding up the “good” side of the equation.

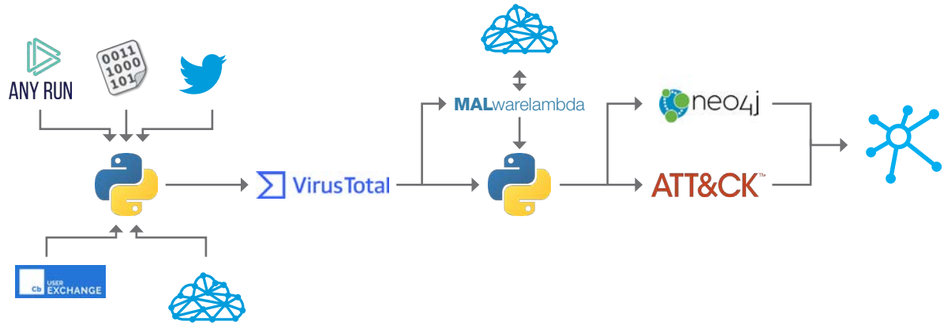
Our goal is to offer a holistic view of how attackers have evolved, what defenders are doing to keep pace, and how security and IT teams can work together in 2020 and beyond in the unending battle of “good vs. evil.”

Research Methodology

For this year’s research, VMware Carbon Black expanded its data set in order to offer a more comprehensive view of the attack landscape. Unless specifically noted in a corresponding section or graphic, the data set analyzed incorporates original threat data composed of: the VMware Carbon Black Cloud customer footprint; the VMware Carbon Black User Exchange; publicly available samples and detonations; VMware Carbon Black Endpoint Standard results, cross-referenced with internally developed tools and SIEMs; and original dark web research. In total, we analyzed 2,000 samples.

These samples were analyzed and graphed using the MITRE ATT&CK™ framework to determine common TTPs in relation to MITRE ATT&CK™ TIDs, ascertained in the most commonly-observed malware classifications of 2019. This was especially the case when considering commodity malware and ransomware samples. Data was gathered, tagged, organized, and systematically detonated using live and static analysis to extract relevant MITRE ATT&CK™ data. Our goal was to better understand the most common techniques for each malware category, determine where they overlap, and improve security efficacy through increased focus on high-value tactics and procedures

Data Sources for Section 01



Malware Supply

- VMware Carbon Black Cloud
- VMware Carbon Black User Exchange
- AnyRun Public Sandbox
- TotalHash
- Twitter Scraping
- VirusTotal

Hash Processing & Normalization to SHA256

- Tag, Organize, and Convert Samples
- Validate all Samples

Categorization anbd Dynamic Detonation

- Ensure All Samples Exist in Database
- Detonate Samples
- Capture Static & Dynamic Data
- Utilize Internal Malware Analysis Environments Within MalwareLambda
- Analyze Telemetry & Behavioral Data from VMware Carbon Black Cloud

Data Processing & Analytics Output

- Correlate All Collected Data to MITRE ATT&CK and Associate Behavioral Data to Relevant TIDs
- Visualize & Correlate Relational Data With Neo4j

Malware Profiles Mapped to MITRE ATT&CK

- Analyze Collected Data
- Extrapolate Commonality of TIDs in Relation to Malware Family
- Utilize Data to Improve Security Efficancy

In Section II of this report: “Defender Behaviors” VMware Carbon Black utilized the results of a commissioned study conducted by Forrester Consulting on a 624 person survey (IT / security manager and above, including CIOs and CISOs) to explore the current state of IT & security relationship dynamics from the C-level to the practitioner level, and how these will evolve. Research for Section II of this report also included qualitative interviews with CIOs and CISOs with responsibility for security strategy and decision making.

Key Report Stats

Attacker behavior continues to become more evasive, a clear sign that attackers are increasingly attempting to circumvent legacy security solutions.

Defense evasion behavior was seen in more than 90% of the 2,000 samples we analyzed.

Ransomware has seen a significant resurgence over the past year.

Defense evasion behaviors continue to play a key role with ransomware (95% of analyzed ransomware samples)

The top industries targeted by ransomware over the past year, according to VMware Carbon Black's global threat data, have been:

- Energy / Utilities
- Government
- Manufacturing

suggesting that ransomware's resurgence has been a nefarious byproduct of geopolitical tension.

Ransomware's evolution has led to more sophisticated Command and Control (C2) mechanisms and infrastructure for attackers. Cyber criminals continue to leverage standard application protocols in network deployments to operate under the radar and blend in with standard business traffic. They are also deploying secondary C2 methods on sleep cycles, allowing them to wake up a new method of C2 upon discovery or prevention of their primary method.

Wipers continue to trend upward as adversaries (including Iran) began to realize the utility of purely destructive attacks. Leveraging techniques across the full spectrum of MITRE ATT&CK™

Wipers rely heavily upon Defense Evasion techniques to avoid detection (64% of analyzed samples).

Classic malware families have spawned the next generation. Throughout our research, we analyzed malware (such as NotPetya) that initially appeared to be ransomware, but upon further inspection, found the decryption component removed or ineffective, resulting in purely destructive malware.

Emotet, once the gold standard for banking Trojans, is being retooled as a Swiss Army knife for modern attackers and is heavily leveraged to perform a myriad of additional attacks due to its modular framework.

IT and security teams appear to be aligned on goals (preventing breaches, efficiency, incident resolution)

but 77.4% of survey respondents said IT and security currently have a negative relationship, according to our study conducted by Forrester Consulting.

55% of survey respondents said driving collaboration across IT and security teams should be the one of the organization's top priorities over the next 12 months, according to the study.

NEARLY 50% **of both IT and security respondents reported being understaffed with security respondents noting their teams are currently 48% understaffed, on average, and IT teams are 26% understaffed, on average, according to the study.**

The study found that, in the majority of cases **45%** the CISO is reporting to the CIO. However, when asked whom the CISO should report to, the majority of respondents **37%** said directly to the CEO. Of note, nearly half **46%** of CIOs said the CISO should report directly to the CEO.

The talent gap continues to be a theme across the IT and security landscape. According to the study,

79% of respondents said finding the right security talent is either "very challenging" or "extremely challenging"

&

70% reported the same level of challenge for IT talent.

MORE THAN 55% **of survey respondents said that both security and IT will share responsibility for key areas like endpoint security, security architecture, and identity and access management over the next three to five years.**

When it comes to risk, **security leaders said brand protection (81% of respondents) is the most important issue for company boards**, according to our study.

Both security and IT have seen increased investments over the last year. Among survey respondents, **77% said they purchased new security products, 69% reported an increase in security staff and 56% reported an increase in IT staff.**

SECTION 01

Attacker Behavior

About the MITRE ATT&CK™ Framework

In 2018, MITRE launched its ATT&CK™ Framework with the intent of "better detection of post-compromise cyber adversary behavior."

MITRE ATT&CK™ redefined not only the phases of attacks but also showed how adversaries could and do behave. In the years that followed, MITRE ATT&CK™ has had a major impact on the cybersecurity industry. It has allowed teams to peel back the layers of an attack and understand how these behaviors occur over time.

MITRE ATT&CK™ continues to change how we design, test and tune our cybersecurity stack. We must continue to evolve our defenses rapidly to keep up with the ever-growing sophistication of cyberattackers. MITRE ATT&CK™ has allowed defenders to focus on a haystack. However, defenders are still asked to determine whether they can find the needle. We believe our research will allow defenders to find that needle faster.

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCerts DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spear Phishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution Through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spear Phishing via Service	Execution Through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Other Physical Medium	Inhibit System Recovery

Click here to view the entire MITRE ATT&CK™ framework.

Top Malware Behaviors of 2019

Attacker behavior continues to evolve and become more evasive.

Over the past year, the most common behaviors seen across all attack data mapped to the MITRE ATT&CK™ Framework were:

26% Software Packing for Defense Evasion

22% Hidden Windows for Defense Evasion

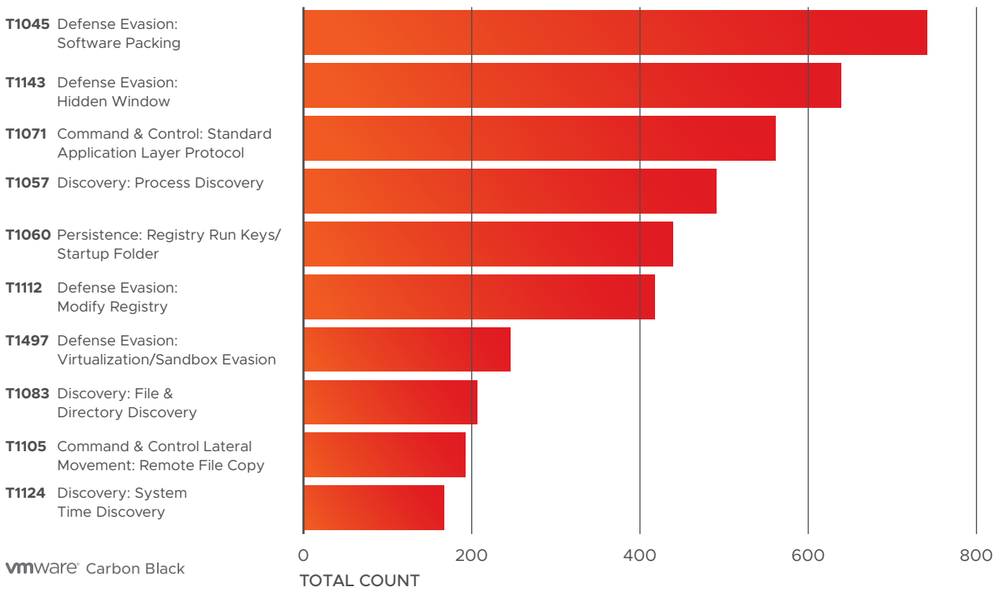
20% Standard Application Layer Protocol for Command & Control (C2)

17% Process Discovery

15% Registry Run Keys in the Startup Folder for Persistence

Of note, evasion behaviors appeared in 90% of the samples we analyzed, a clear indication that attackers are increasingly attempting to circumvent legacy security solutions.

Top 10 Malware Behaviors of 2019



Behavior Spotlights

Software Packing

Advice to Defenders

According to MITRE, Software Packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Utilities used to perform software packing are called packers. Software Packing also includes custom encoding/compression/ encryption schemes that are routinely used by droppers or installers which are common in commodity and targeted attacks.

Defenders should look to thin out their attack surface wherever possible. Use solutions that allow you to analyze endpoints for software packers or evidence that packers were used. Getting to know the normal applications that employ this technique will help quell any noise from false positives to help the team focus. Point-in-time security solutions will offer little coverage for software packing. Employing an EPP that records and analyzes data over time is helpful in preventing and detecting these types of attacks.

Defensive Evasion Hidden Window

Advice to Defenders

According to MITRE, Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling / disabling security software or obfuscating / encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware.

Adversaries may implement hidden windows to conceal malicious activity from the plain sight of users. In some cases, windows that would typically be displayed when an application carries out an operation can be hidden. This may be utilized by system administrators to avoid disrupting user work environments when carrying out administrative tasks. Adversaries may abuse operating system functionality to hide otherwise visible windows from users so as not to alert the user to adversary activity on the system.

Once again, attackers have shown that they will and are using system tools and techniques that are generally provided for system administration purposes.

Limit or restrict program execution using EPP or Application Whitelisting. On MacOS, whitelist programs that are allowed to have the plist tag. All other programs should be considered suspicious.

Monitor processes and command-line arguments for actions indicative of hidden windows with EDR. In Windows, enable and configure event logging and PowerShell logging to check for the hidden-window technique. Understand that obfuscation and encoding of PowerShell attacks is a very common tactic, utilized by various malware families to evade defenses. Many such attacks can even disable PowerShell logging and related defensive tools,so ensure that you use a layered approach to your overall security program.

In MacOS, PLIST files are ASCII text files with a specific format, so they're relatively easy to parse. File monitoring can check for the apple.awt.UIElement or any other suspicious PLIST tag in PLIST files and flag them.

Resurgent Ransomware & Evolving Behaviors

In security, 2016 was "The Year of Ransomware." Since then, ransomware has only gotten more pervasive, costing billions in damages. 2019 could have been referred to as "The Year of Ransoming Governments."

Among the Notable Attacks:

113 State and Municipal Governments and Agencies

764 Healthcare Providers

89 Universities, Colleges and School Districts

VMware Carbon Black has observed an increased rise not only in the number of ransomware variants but also new ransomware behaviors witnessed on a recurring basis. The most common behaviors seen across all ransomware attack data mapped to the MITRE ATT&CK™ Framework were:

29% Hidden Windows for Defense Evasion

20% Software Packing for Defense Evasion

19% Process Discovery

17% Registry Run Keys in the Startup Folder

15% Standard Application Layer Protocol for Command and Control (C2)

Of note, defense evasion behaviors continue to play a key role with ransomware. We saw that behavior in 95 percent of our analyzed ransomware samples.

Ransomware's resurgence played out across the vertical landscape in 2019. Looking at the data, it's hard to ignore the role geopolitical tension has played in this resurgence with the most targeted verticals of the year being:

32% Energy / Utilities

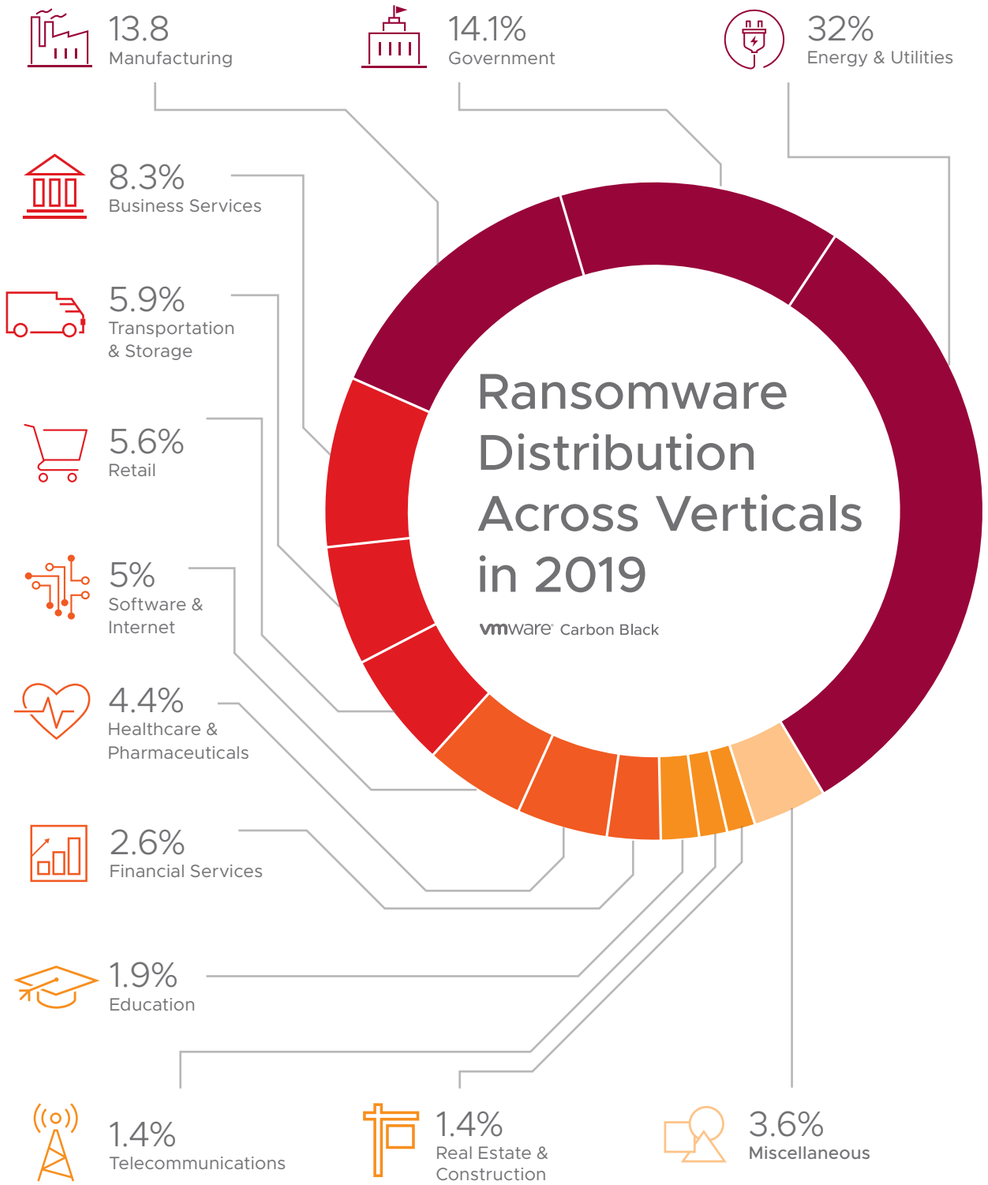
14.1% Government

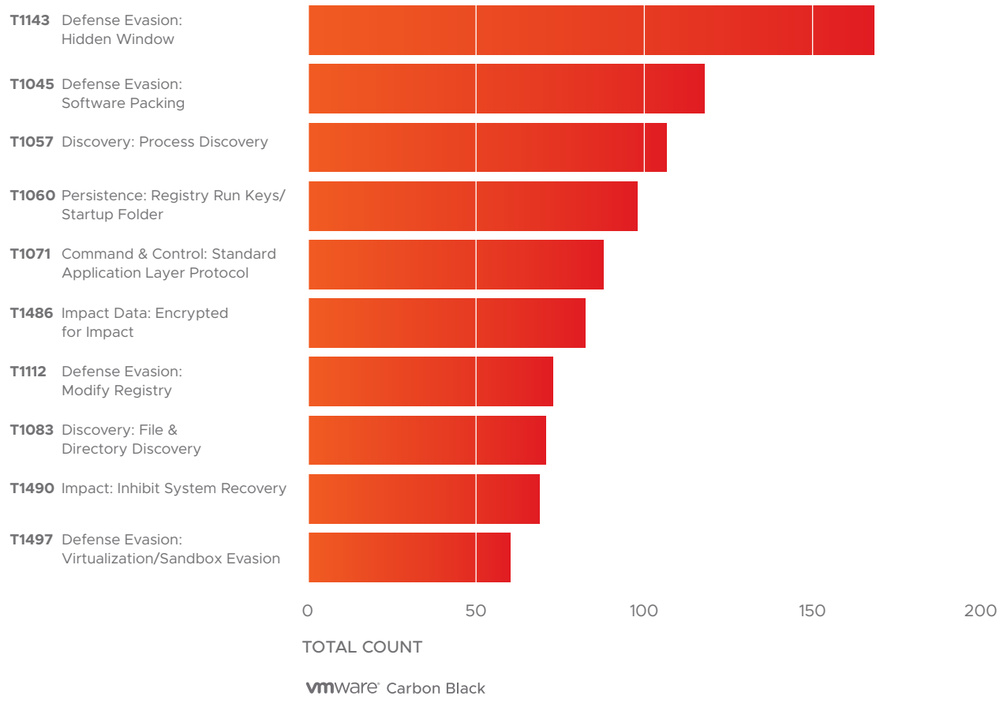
13.8% Manufacturing

The clear spike in both Energy / Utilities and Government suggests that as geopolitical tensions rise so do attacks on these sectors, which often serve as critical infrastructure and provide critical services to massive portions of the population.

Ransomware continues to be used illicitly to gain cryptocurrency, which is being used by nation states to bypass sanctions. In September 2019, the ***U.S. Treasury Department stated*** that state-sponsored hacking groups from North Korea attacked critical infrastructure, drawing illicit funds that ultimately funded the country's weapons and missile programs. These attacks remain generally low cost to perform with a high rate of return. In this cyber arms race, when nation states are involved, the evolution of malware speeds up. We should expect to see a continual arms race for extortion. For nation states, ransomware can be an effective tool to gain returns on an investment. And just like all other malware scoped as part of this research, ransomware is continually evolving.It is being used to gain a footprint onto a system. It is being used to create noise and distract defenders. Ransomware can and will continue to make a great ruse while more nefarious activity occurs.

Ransomware attacks will continue to be aimed at sectors which have historically struggled to defend their systems. Ransomware as a service provider continues to gather data on vertical's pay rates and how fast the victim paid. These will be used to not only lower their cost of delivery and maximize profits but also to help target future attacks, such as access mining and crypto-jacking.


13.8
Manufacturing
14.1%
Government
32%
Energy & Utilities
8.3%
Business Services
5.9%
Transportation
& Storage
5.6%
Retail
5%
Software &
Internet
4.4%
Healthcare &
Pharmaceuticals
2.6%
Financial Services
1.9%
Education
1.4%
Telecommunications
1.4%
Real Estate &
Construction
3.6%
Miscellaneous
Ransomware
Distribution
Across Verticals
in 2019
vmware Carbon Black


Top 10 Ransomware Behaviors of 2019
T1143 Defense Evasion:
Hidden Window
T1045 Defense Evasion:
Software Packing
T1057 Discovery: Process Discovery
T1060 Persistence: Registry Run Keys/
Startup Folder
T1071 Command & Control: Standard
Application Layer Protocol
T1486 Impact Data: Encrypted
for Impact
T1112 Defense Evasion:
Modify Registry
T1083 Discovery: File &
Directory Discovery
T1490 Impact: Inhibit System Recovery
T1497 Defense Evasion:
Virtualization/Sandbox Evasion
0
50
100
150
200
TOTAL COUNT
vmware Carbon Black


T1057
T1060
T1071
T1112
T1083
T1490

Ransomware TTPs Overlayed on the MITRE ATT&CK™ Framework

This chart highlights the various MITRE ATT&CK™ TTPs associated with ransomware.

- The red boxes highlight instances where the TTP was observed.
- Orange highlights TTPs that were observed across multiple high-level tactics.

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT
	Scripting	Hidden Files & Directories	New Service	Virtualization / Sandbox Evasion	Input Capture	Virtualization / Sandbox Evasion	Remote File Copy	Input Capture	Remote File Copy		Data Encrypted for Impact
	Scheduled Task	New Service	Scheduled Task	Hidden Files & Directories	Hooking	Process Discovery		Data from Local System	Standard Application Layer Protocol		Inhibit System Recovery
	Windows Management Instumentation	Scheduled Task	Hooking	Scripting	Credentials in Files	File and Directory Discovery		Automated Collection	Standard Cryptographic Protocol		Data Destruction
	Command-line Interface	Hooking	Service Registry Permissions Weakness	Hidden Window		System Time Discovery		Data from Network Shared Drive	Multilayer Encryption		Defacement
		Service Registry Permissions Weakness		Software Packing		System Network Configuration Discovery		Clipboard Data	Multi-hop Proxy		Service Stop
		Registry Run Keys / Startup Folder		Modify Registry		Query Rigistry					
		Bootkit		NTFS File Attributes		System Network Connections Discovery					
				Masquerading		System Information Discovery					
				File System Logical Offsets		Network Share Discovery					
				Obfuscated Files or Information		Security Software Discovery					
				Rootkit		Application Window Discovery					
				Disabling Security Tools							
				Indicator Removal on Host							
				File Deletion							

Ransomware Behavior Spotlight

Standard Application Layer Protocol

According to MITRE, ***adversaries may communicate*** using a common, standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid detection by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are RPC, SSH, or RDP.

Advice to Defenders

To understand the full picture of C2, as well as to combat the rising phenomenon of multiple C2 channels on sleep cycles, defenders will need to fuse both EDR data as well as network data sources such as: DNS logs, full packet capture, Internet and firewall logs. Defenders should look to interpret C2 as soon as possible to prevent further damage but also be weary of secondary C2 channels that wake up when defenders take action against the primary C2 method. Limit or disable outbound server communications to only ones needed. Do not narrowly focus on any one TID; rather, **focus on the cluster and broader behaviors of how destructive attacks enter and execute in your environment.**

Destructive Attack Behaviors

According to the latest *VMware Carbon Black Global Incident Response Threat Report (GIRTR)*, leading incident response professionals reported experiencing destructive / integrity impact in 41 percent of attacks. This marks a 10 percent increase over the prior two quarters and an ominous trend as cyberspace is becoming more punitive. Destructive cyberattacks have a notorious history including high-profile attacks against the Siberian Pipeline, resulting in one of the world's largest non-nuclear explosions; Dark Seoul; Stuxnet; Black Energy; and NotPetya.

History of Destructive Cyberattacks

Subset of High Profile, Public, and Documented Destructive Attacks

PHYSICALLY DESTRUCTIVE DESTRUCTIVE

1982 – Siberian Pipeline
The CIA tricked the Soviet Union into acquiring ICS software with built-in flaws. Software was programmed to malfunction - resulting in one of the worlds largest non-nuclear explosions.

1998 – Kosovo
35,000 computers wiped and replaced with burning American flag by Iranians.

1998 – CIH
Chernobyl virus which overwrote critical systems data – affecting 60-million computers. Developed by a Taiwanese student.

2008 – Georgia
Russian Joint campaign against Gorgian targets. Website defacement, DDos, and diverting citizens web traffic through Russia.

2008 – Beijing Olympics
Deceptive Russian Campaign to disrupt the Olympic Games.

2010 – Stuxnet
US and Israeli developed-malware leveraged to delay the Iranian Nuclear Program's ability to enrich Uranium. The malware targeted Siemens ICS and physically destroyed Uranium centerifuges, leveraging 4 zero-days.

2013 – Dark Seoul
North Korean attacks on South Korean Television Stations and Banks.

2014 – Sony Entertainment
Norght Korean attack in response to movie – data theft and wiping resulting in $35 million in damages.

2014 – German Steel Mill
Attack on ICS controlling blas furnace, resulting in significant physical damage.

2015 – TV5Monde
Russian actors destroyed French TV station hardware, taking the network offline for 12-hours.

2015 – Black Energy
Russian attack on three Ukrainian Energy Distrubution Companies. Cutting power to 225,000 civilians.

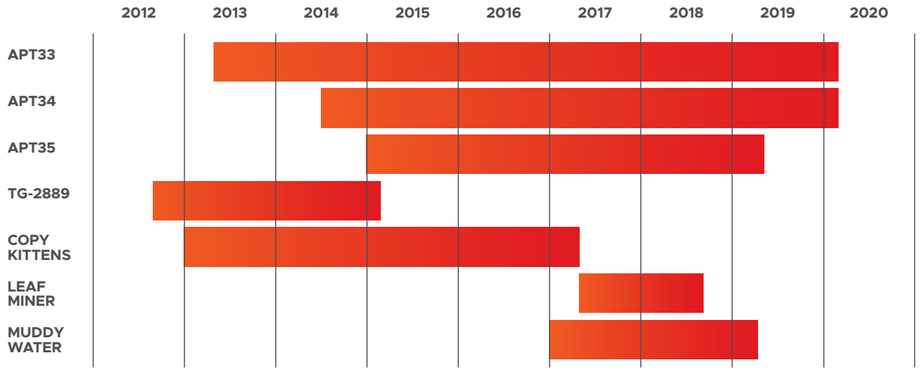
2016 – Crash Override
Russian attack on electric transmission station ICS system in Kiev, Ukraine.

2017 – NotPetya
One of the most damaging Cyber Attacks in history. Russia targeted large Ukraine companies. Estimated to have cost over $10 Billion in damages, globally.

Dustman & Iran's Rising Destructive Cyberattack Capability

The *VMware Carbon Black Threat Analysis Unit (TAU) recently performed* a deep dive into Iran's resurging destructive cyberattack capability.

Traditionally, there have been several high-profile threat groups suspected to have been backed by or acted on behalf of Iran. Using the below image as a high level timeline, we can see these Iranian threat groups have been active in cyberattacks for a considerable amount of time. The recent tensions in the Middle East region have brought this threat to the forefront in the news. While the threat and capabilities of groups supporting Iran are very real, they have not just become active with the activity that has occurred recently. From public reporting and internal research, many of these groups rely heavily on common tactics like spear phishing, brute force attacks, and internet facing systems with unpatched known vulnerabilities.



Defender Advice

Detecting and stopping these attacks in the earliest stages should continue to be a principle that security teams continually refine in their organizations. Cyber criminals continue to refine their techniques. Defenders must counter this by having a program that focuses on continuous improvement. Focusing on spear phishing, user execution, credential dumping, and living-off-the land techniques will yield positive security returns that will help combat numerous threat groups and malware families.

Wiper Behaviors

Wipers continue to trend upward as adversaries (including Iran) began to realize the utility of purely destructive attacks. Leveraging techniques across the full spectrum of MITRE ATT&CK™, wipers rely heavily upon Defense Evasion techniques (64 percent of analyzed samples).

The most common behaviors seen across all wiper attack data mapped to the MITRE ATT&CK™ Framework were:

33% Data Destruction

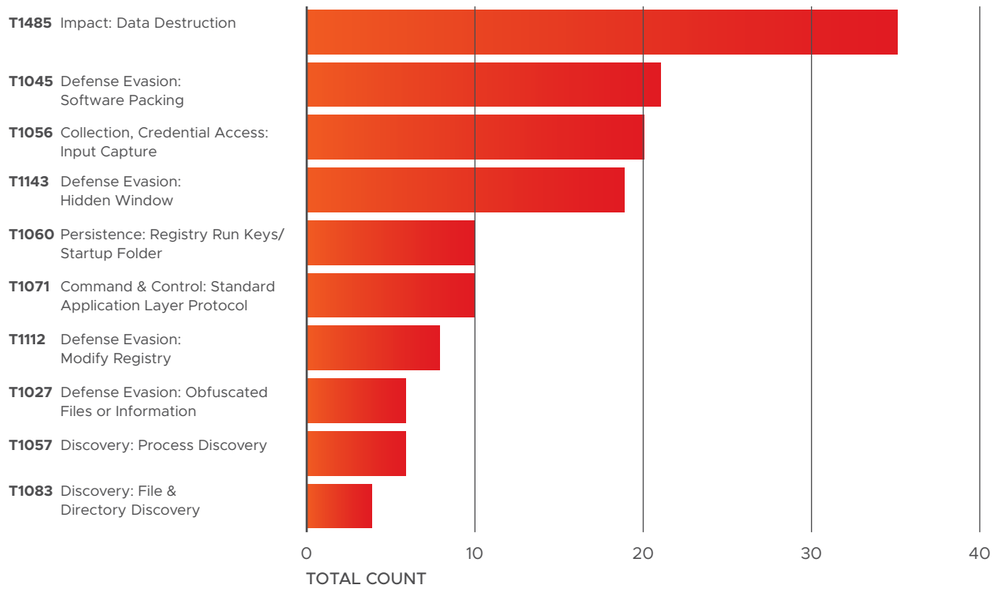
20% Software Packing for Defense Evasion

19% Input Capture for Collection & Credential Access

18% Hidden Windows for Defense Evasion

10% Registry Run Keys in the Startup Folder for Persistence

Top 10 Wiper Behaviors of 2019



Wiper TTPs Overlayed on the MITRE ATT&CK™ Framework

This chart highlights the various MITRE ATT&CK™ Techniques Tactics and Procedures associated with malware generally classified as wipers.

- The red boxes highlight instances where the TTP was observed.
- Orange highlights TTPs that were observed across multiple high-level tactics.

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT
	Scheduled Task	Hidden Files & Directories	New Service	Process Injection	Input Capture	Process Discovery	Remote File Copy	Input Capture	Remote File Copy		Data Destruction
		New Service	Scheduled Task	Hidden Files & Directories	Hooking	File and Directory Discovery		Data from Local System	Standard Application Layer Protocol		Defacement
		Scheduled Task	Hooking	Hidden Window	Credentials in Files	System Network Configuration Discovery		Automated Collection	Standard Cryptographic Protocol		
		Hooking	Process Injection	Software Packing		Query Registry					
		Registry Run Keys / Startup Folder		Modify Registry		System Network Connections Discovery					
		Bootkit		NTFS File Attributes		System Information Discovery					
				Masquerading		Network Share Discovery					
				File System Logical Offsets							
				Obfuscated Files or Information							
				Rootkit							
				Disabling Security Tools							

Wiper Behavior Spotlights

Data Destruction

According to MITRE, adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives. It may have worm-like features to propagate across a network by leveraging additional techniques like Valid Accounts, Credential Dumping, and Windows Admin Shares.

Advice to Defenders

First and foremost, defenders should ensure that IT-hygiene basics are done and tested on a regular basis. Having a strong and tested disaster recovery plan will help shepherd you through a lot of the worst-case cyber scenarios out there. Having strong IT practices like snapshots, redundant systems, and Application Whitelisting in place will put you in a better position should someone try to use a wiper against you. Behavioral-based EPP is also recommended. Having an EDR component focused on east-west traffic will help detect this behavior. Strong micro-network segmentation will help to stop any lateral movement component of these attacks.

Malware's Continued Evolution

Access Mining Evolves

A recent example of malware evolution is Access Mining, a tactic where an attacker leverages the footprint and distribution of commodity malware, in this case a cryptominer, using it to mask a hidden agenda of selling system access to targeted machines on the dark web.

In 2019, ***VMware Carbon Black's Threat Analysis Unit*** uncovered a secondary component in a well-known cryptomining campaign. The malware had been enhanced to exfiltrate system access information for sale on the dark web. This discovery indicated a bigger trend of commodity malware evolving and will likely catalyze a change in the way cybersecurity professionals classify, investigate, and protect themselves from commodity threats.

Advice to Defenders

Attackers are not leaving. Cyber criminals have moved from burglaries and break-ins to full on occupations and cyber real estate sales. It remains critical that attacker behavior be recorded and analyzed over time to reveal those still lurking in the dark.

VMware Carbon Black TAU Analysis: Emotet

Emotet is a family of banking malware, which has been around since at least 2014. Attackers continue to leverage variants of Emotet and are becoming increasingly shrewd in the techniques they employ to deliver the malware onto an infected system. VMware Carbon Black's TAU and other researchers observed the adaptation to existing methods leveraging PowerShell, where attackers were encrypting the URLs of the C2 servers used to host the second stage payload. A spike in this type of evolution has been observed over the last two years.

Cybercriminals can leverage Emotet's capabilities to gain initial access, steal sensitive information, and even perform more destructive attacks such as executing ransomware or wiping capabilities, all while moving laterally via Eternal Blue and related spreading mechanisms.

For more on Emotet, click here.

SECTION 02

Defender Behavior

Security is a team sport, or at least it should be. Given the constant behavior evolution we see from attackers and the vast IT footprint attackers can target, IT and security teams clearly face an uphill battle. Whereas attackers only have to be right once to succeed, defenders must be right 100 percent of the time. To reach that level of success, prioritizing the right people, processes, and technology is critical. To determine how well IT and security are working together, VMware commissioned Forrester Consulting to explore the current state of the IT / security relationship dynamics (from the C-level to practitioners) and how these dynamics will evolve.

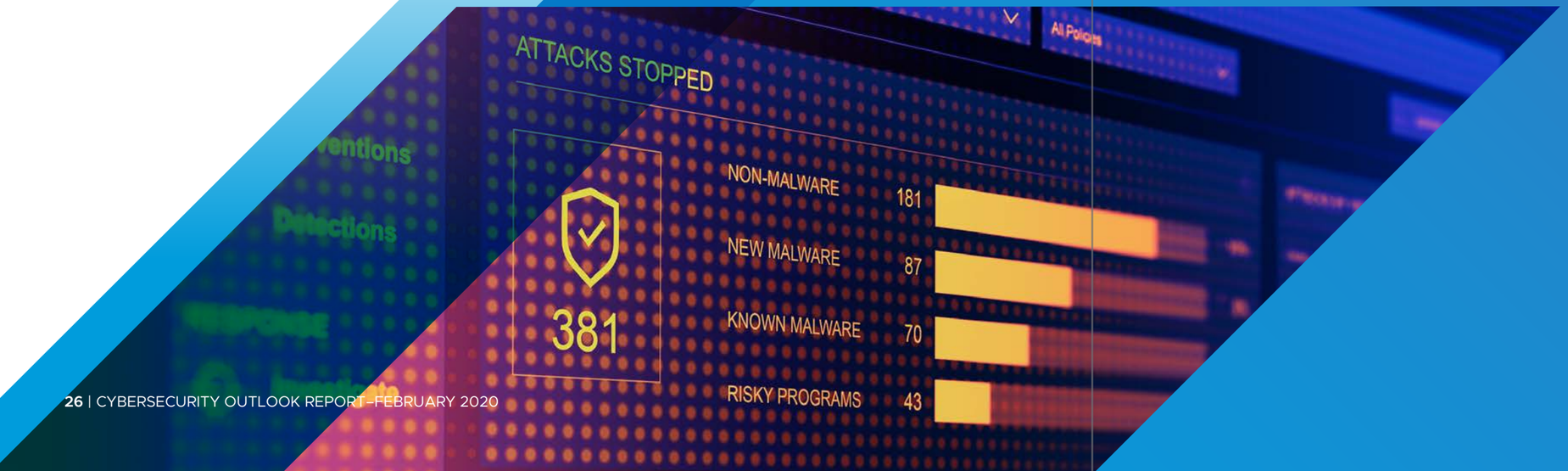
THE STUDY TESTED THE FOLLOWING HYPOTHESIS:

Some organizations have misaligned priorities between IT and security teams, often driven by process and organizational challenges including discrepancies among reporting structures, budgets, processes, or skill sets. In light of the security talent shortage, organizations must play security as a team sport to best defend against cyberattacks.

Executing against a consolidated IT management and security strategy will help break down silos.

Despite inherent differences in the teams, a common strategy can empower both security and IT to enable effective risk mitigation, continuous compliance, and improved threat response workflows that decrease time to detection and containment without sacrificing infrastructure or business agility.

Forrester's global survey across APAC, EMEA, and North America includes responses from 624 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making. Qualitative interviews were also conducted. Survey respondents came from a number of verticals, including: technology, finance, healthcare, retail, and education/non-profits.



Expectations vs. Reality & Existing Tension

An initial positive sign is that strategic priorities between IT and security are fairly aligned, with preventing breaches, efficiency, and incident resolution among the top goals for today's teams.

Rank the Top 3 Priorities for Your Team.*

Top 3 **IT** Priorities

1. Preventing Data Breaches | **54%**
2. Efficiency | **53%**
3. Incident Resolution | **45%**

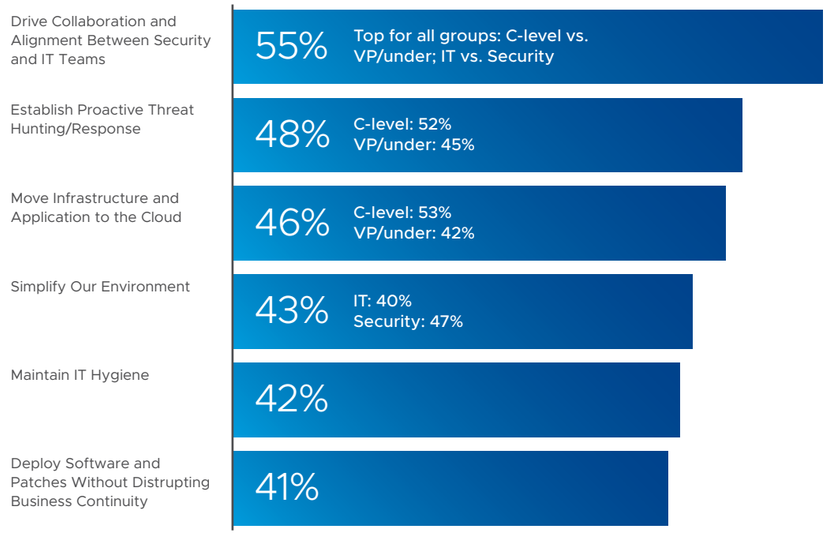
Top 3 **Security** Priorities

1. Efficiency | **58%**
2. Preventing Data Breaches | **54%**
3. Incident Resolution | **42%**

*Source: a commissioned study conducted by Forrester Consulting on behalf of VMware, January 2020

A more comprehensive look at organizational priorities provides a deeper look. According to the study, "driving collaboration and alignment between security and IT teams" topped the list with 55 percent of respondents listing it as a top organizational priority over the next 12 months.

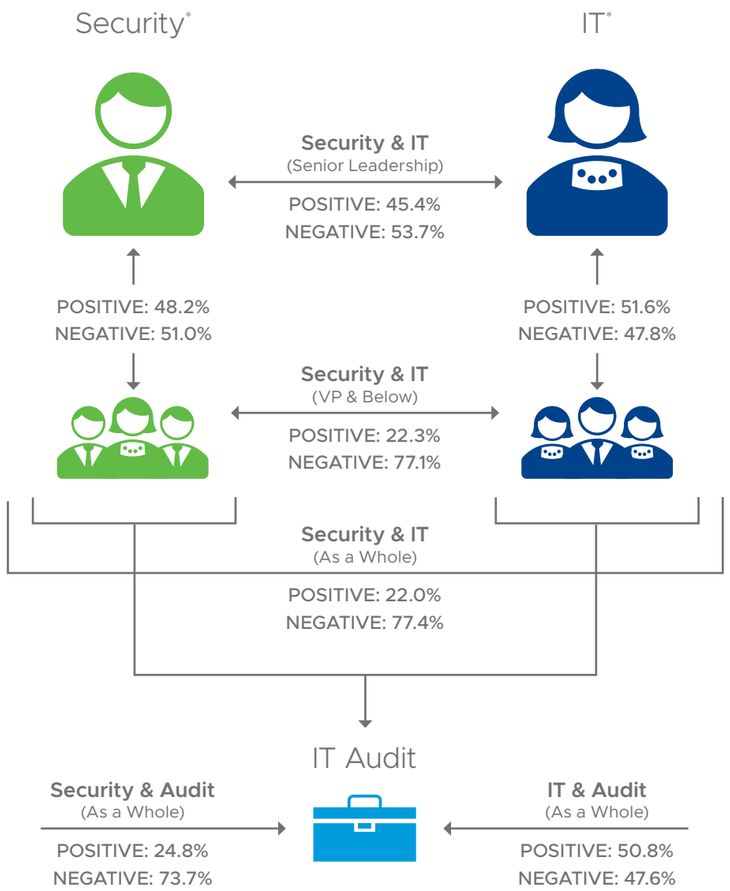
Which of the Following Initiatives Are Likely to be Your IT Organization's Top Priorities Over the Next 12 Months? Top 6 Shown. Additional Options in Appendix.*



Given this clear prioritization, there's potential cause for concern when looking at the data surrounding the existing relationships between IT and security teams and leaders.

*Source: a commissioned study conducted by Forrester Consulting on behalf of VMware, January 2020

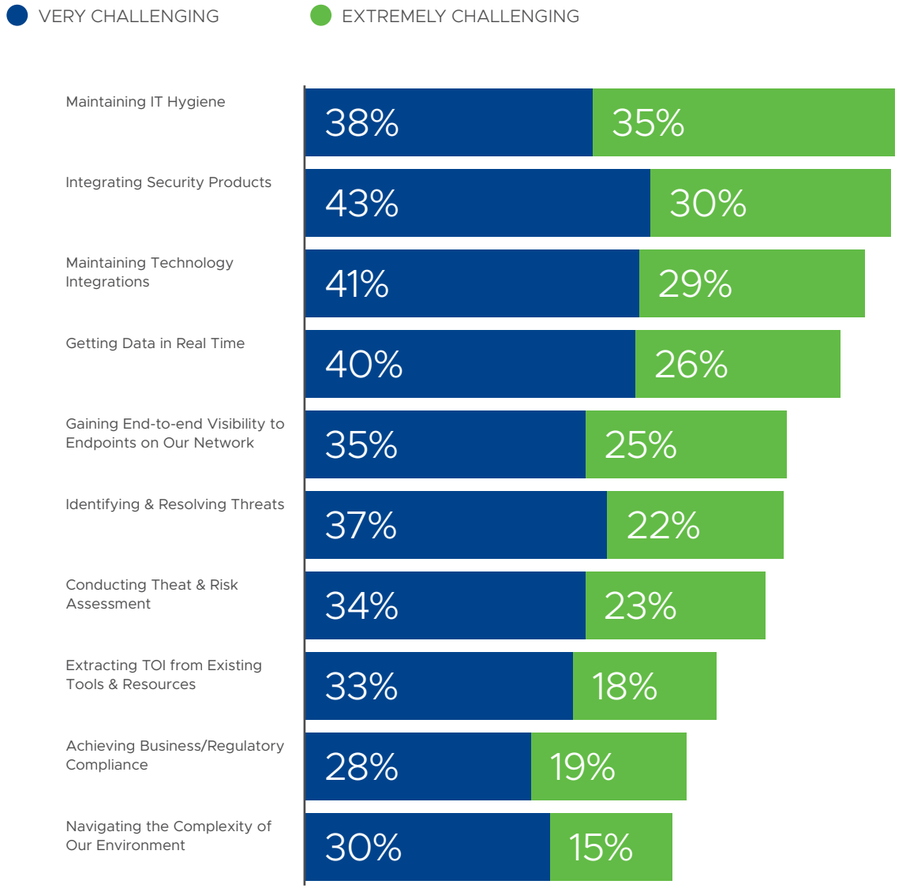
According to the study, 77.4 percent of respondents noted that IT and security had a negative overall relationship. Among senior leaders, 53.7 percent noted the relationship between the CIO and CISO was negative, suggesting existing tension. The rest of the numbers are equally as sobering as the only relationships with majority positive numbers were "CIO with VP and below" and "IT with audit" within the IT organization. According to the data, there's some work to be done.



*Source: a commissioned study conducted by Forrester Consulting on behalf of VMware, January 2020

Existing IT / security challenges extend beyond personnel relationships. Maintaining IT hygiene, integrating security products and maintaining technology integrations contribute to potential issues and topped the study's list as some of the most concerning issues for survey respondents.

How Challenging Do You Find the following IT and Security Tasks?*



*Source: a commissioned study conducted by Forrester Consulting on behalf of VMware, January 2020

Staffing & Resource Concerns

According to the study, staffing resources and structure may be playing a role in the IT / security tension. Nearly 50 percent of both IT and security respondents reported being understaffed with security respondents noting their specific teams are, on average, 48 percent understaffed and IT teams are, on average, 26 percent understaffed.

Does Your Team Have Adequate Staff?*

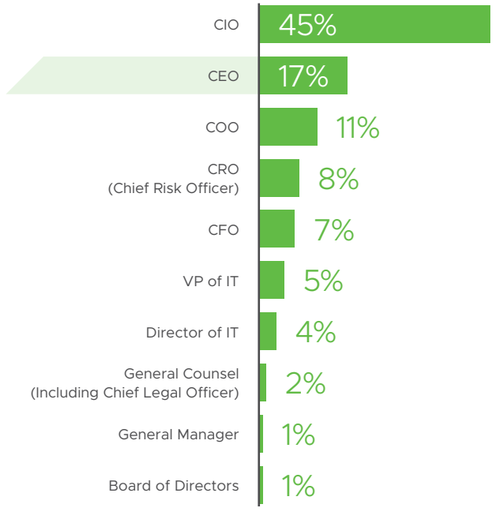
Security		IT	
49%	Understaffed *Average Team Understaffed by 48%*	49%	Understaffed *Average Team Understaffed by 26%*
36%	Adequately Staffed	39%	Adequately Staffed
6%	Overstaffed	7%	Overstaffed
9%	Don't Know	4%	Don't Know

This issue is further magnified by the C-suite's current perception of IT and security staffing. Only 31 percent of C-suite respondents said their IT and security teams are understaffed while 61 percent of VP-and-below respondents said these teams are understaffed. This 30-point delta suggests that the C-suite may be out of touch with the day-to-day IT and security resourcing needs for the organization.

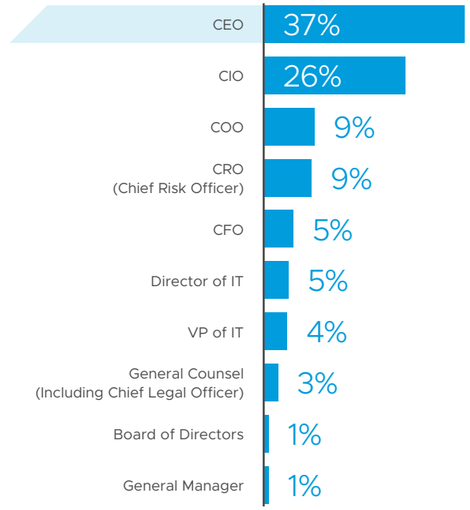
*Source: a commissioned study conducted by Forrester Consulting on behalf of VMware, January 2020

Reporting structures may also need modifications. In the majority of cases (45 percent) the CISO is reporting to the CIO. However, when asked who the CISO should report to, 37 percent of respondents said directly to the CEO. This issue is further clouded when examining the specific responses from CIOs and CISOs.. Nearly half (46%) of CIOs said the CISO should report directly to the CEO. Among CISOs, the study saw an even split - 31 percent of CISOs said the CISO should report to the CIO and 31 percent of CISOs said the CISO should report to the CEO.

Our CISO Currently Reports to:*

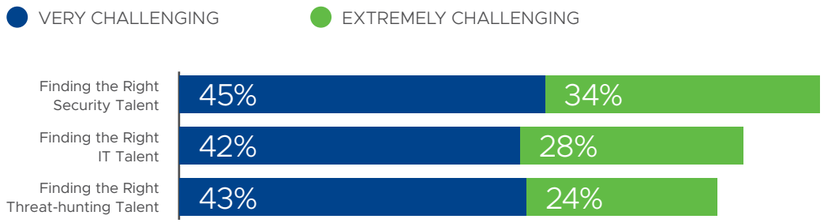


Our CISO Should Report to:*



Of course, IT and security talent is often hard to come by, with security being a bit more challenging, according to the study results. 79 percent of respondents said finding the right security talent is either "very challenging" or "extremely challenging" and 70 percent reported the same for IT talent.

How Challenging Do You Find the following IT and Security Tasks?*



*Source: a commissioned study conducted by Forrester Consulting on behalf of VMware, January 2020

Security as a Team Sport

Executing a consolidated IT management and security strategy will help break down silos and empower respective teams to tackle security as a team sport. As noted above, respective priorities are well aligned, and the desire to reduce risk travels all the way up to the board of directors.

Paramount to risk reduction and better alignment is the ability to drive collaboration and share decision making. To that end, It's not surprising that more than 50 percent of survey respondents said that both security and IT will share responsibility for areas like endpoint security, security architecture, and identity and access management over the next three to five years. We view that as a positive sign for the near future. IT and security professionals alike are optimistic that shared responsibility will become the norm and, perhaps, drive better alignment across many critical areas of the business.

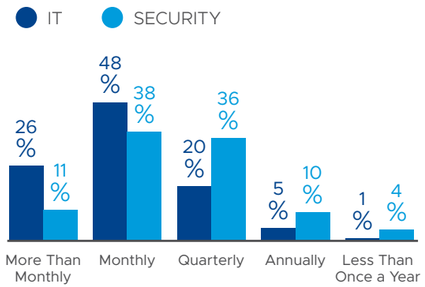
Which Team is Currently the Primary Decision Maker for the Following Categories? Which Team do You Think will be the Primary Decision Maker for the Following Categories in 3 to 5 Years?*

	NOW Both Teams Share Responsibility	3-5 YEARS Both Teams Share Responsibility	DELTA	NOW IT	3-5 YEARS IT	DELTA	NOW Security	3-5 YEARS Security	DELTA
IT Securitys Architecture	21.2%	53.5%	32.3%	21.3%	24.8%	3.5%	55.8%	18.8%	-37.0%
Endpoint Security	21.6%	53.4%	31.8%	30.4%	22.4%	-8.0%	44.7%	20.8%	-23.9%
Identity & Access Management	27.4%	56.9%	29.5%	34.1%	26.9%	-7.2%	34.9%	13.3%	-21.6%
Application Modernization	27.4%	52.7%	25.3%	38.3%	29.6%	-8.7%	30.3%	13.3%	-17.0%
Cloud Security	22.4%	44.6%	22.2%	24.8%	32.2%	7.4%	50.0%	20.2%	-29.8%
Threat Hunting/Remediation/ Incident Response	18.4%	40.4%	22.0%	25.0%	30.0%	5.0%	53.4%	26.3%	-27.1%
Network Security	21.8%	42.8%	21.0%	26.3%	23.6%	-2.7%	48.9%	30.1%	-18.8%
Third-party IT Services	23.4%	43.4%	20.0%	55.1%	38.9%	-16.2%	17.0%	14.6%	-2.4%
Security Policies	27.6%	40.1%	12.5%	19.4%	22.4%	3.0%	49.2%	35.3%	-13.9%
Virtualization	26.3%	36.4%	10.1%	56.6%	46.2%	-10.4%	13.0%	13.0%	0.0%
Workloads & Workload Protection	35.1%	41.5%	6.4%	41.7%	36.5	-5.2%	20.7%	18.3%	-2.4%
IT Tool/Technology Selection	28.0%	33.3%	5.3%	57.5%	51.4%	-6.1%	11.5%	12.2%	0.7%
Mobile Device Management	32.1%	37.3%	5.2%	50.3%	47.3%	-3.0%	14.1%	11.4%	-2.7%
Cloud Infrastructure	28.0%	32.1%	4.1%	34.6%	38.9%	4.3%	32.5%	25.0%	-7.5%
Hordware Infrastructure	30.9%	33.0%	2.1%	51.1%	48.2%	-2.9%	14.3%	14.4%	0.1%

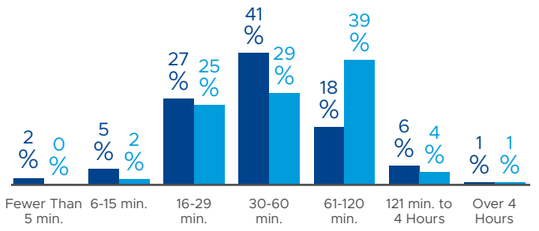
*Source: a commissioned study conducted by Forrester Consulting on behalf of VMware, January 2020

The data also shows greater collaboration and visibility on security at the board level compared to two years ago. Security has increasingly become a board-level discussion. Our study shows that both CIOs and CISOs typically meet with the board at least quarterly.. While CIOs tend to meet with boards more frequently, CISOs do so for a longer duration, on average.

How Frequently Do You Meet Directly With Your Board?*



When You Do Meet With Your Board, How Much Time On Average Do You Spend Meeting With Them?*



	Frequency (times per year)	Duration	Avg. Time Per Year
IT	10.1	55.2 Minutes	9.3 Hours
Security	7.7	64.4 Minutes	8.3 Hours

According to the study, boards want a greater understanding of the company's cybersecurity strategy because security has become fundamental to the overall health of the business. Board members want a clear line of sight to potential risks. According to the study, CIOs and CISOs shared that the top two items boards care about most are brand protection and security threats / risks to the business. Unsurprisingly, reducing risk appears to be a common theme.

Based On Your Interactions, How Important Are the Following Items to Your Board? (Top 3 Very Important / Critical Items Shown)*

*Source: a commissioned study conducted by Forrester Consulting on behalf of VMware, January 2020

Budgeting & Investments

As security continues growing in relevance and importance, so have budgets and staff. This may be good news for understaffed security teams. The study found that budgets have increased over the last 12 months for 80 percent of survey respondents.

Both security and IT have seen increased investments over the last year. Among survey respondents, 77 percent said they purchased new security products, 69 percent reported an increase in security staff, and 56 percent reported an increase in IT staff.

Rate Your Level of Agreement With the Following Statements Regarding the Past 12 Month. (% Agree / Strongly Agree Shown)*

81%
We Have Increased our **IT** Budget.

80%
We Have Purchased New **IT** Products.

56%
We Have Increased our **IT** Staff.

80%
We Have Increased our **Security** Budget.

77%
We Have Purchased New **Security** Products.

69%
We Have Increased our **Security** Staff.

*Source: a commissioned study conducted by Forrester Consulting on behalf of VMware, January 2020

Conclusion

Behaviors matter. If 2019 has shown anything, it's that attackers will continue to evolve their behaviors and defenders must respond accordingly.. The trickle-down cyber economy, fueled by nation states and advanced persistent actors, has picked up speed and systems are being brokered out for nefarious purposes.

Attackers are becoming more punitive as demonstrated by the clear rise in ransomware, wipers, and destructive attacks over the year. Attackers have become adept at evading security solutions. Their quality assurance has risen. They have gotten stealthier when it comes to command and control. Organizations find themselves defending against attacks fueled by rising geopolitical tension.

Attackers are not leaving. This is our new reality and we must adjust. As defenders, we must shift not only our thinking but also our people, processes, and technologies to account for new attacker behaviors.

Moving into 2020, it’s not about focusing on one type of attack. Attack types are blending and attackers are learning from each other. In 2020, we should focus more on the attacker behaviors and less on the noise. By focusing on behaviors, teams can move to become proactive and hunt these behaviors before they cause harm.

Our defenses should be informed by each and every attack, allowing our collective defense to rise together. Defenders must stop thinking about how to achieve results on their own. Defenders must continue to build bridges with IT teams. The time for cooperation is now. We can no longer afford to tackle this problem alone. We need IT teams to look toward security solutions that are built in and not bolted on. It’s time for security to become part of our organizational DNA. It’s time security becomes intrinsic to how we build, deploy, and maintain technology.

About VMware

VMware software powers the world's complex digital infrastructure. The company's cloud, networking and security, and digital workspace offerings provide a dynamic and efficient digital foundation to customers globally, aided by an extensive ecosystem of partners. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough innovations to its global impact. For more information, please visit https://www.vmware.com/company.html

vmware® Carbon Black