Advance Your Ransomware Defenses

An Enterprise Guide to Hardening Your Endpoints Against Future Ransomware Attacks
Table of Contents

Executive Summary ........................................................................................................... 3
  An Enterprise Guide to Future-Proofing Ransomware Defenses

History of Ransomware ..................................................................................................... 5
  A Brief History, Stats and Timeline

How Ransomware Works .................................................................................................. 13
  Stages of an Attack

Ransomware Attack Anatomy ............................................................................................ 15

Locky Variant - Shadow Copies ......................................................................................... 17
  Defeating Locky and Volume Shadow Copies

Advance Your Ransomware Defenses ................................................................................ 21

Ransomware Defense Cheat Sheet ...................................................................................... 23
  Defense In Depth: 14 Keys to Protecting Against Ransomware

Case Study - Financial Services ......................................................................................... 25
  Taking Preemptive Action Against Ransomware

Conclusion ............................................................................................................................ 26
  Next Generation Ransomware Prevention
WHILE RANSOMWARE ISN’T GOING AWAY ANY TIME SOON (IF EVER), YOU CAN DEFEND YOUR ORGANIZATION - IF YOU’RE PROPERLY PREPARED.

An Enterprise Guide to Future-Proofing Ransomware Defenses

Ransomware isn’t new. In fact, it’s 30-years-old. What IS new is ransomware’s sudden rise as a favored attack by cyber criminals. Cyber crime has become a lucrative business and, unfortunately, ransomware has become an integral attack method that many organizations are fighting a losing battle against.

Ransomware attackers are implementing new, innovative techniques that employ unknown binaries and non-malware tactics to evade and bypass traditional defenses. Their encryption techniques go beyond simple files and shares to make it even harder to restore using backups. And their primary targets are increasingly becoming organizations (not just individuals), with much more to lose (and more money to payout).

As a result, today’s businesses are routinely choosing to pay hefty ransoms rather than lose access to their intellectual property, patient records, credit card information and other valuable business data. Simply put, targeted businesses are paying ransoms in order to avoid significant disruptions to normal operations.

Ransomware’s rise in popularity parallels the development of fileless attack methods that traditional antivirus (AV) simply cannot stop. Cyber criminals are quick learners and eager to make fast money. Whether extorting $300 per user from a small business, or $30 million from a multinational enterprise, the level of effort is often similar.

While ransomware isn’t going away any time soon (if ever), you CAN defend your organization - if you’re properly prepared.

In this eBook, we answer the questions: “What is ransomware?,” “How does it work?” and “What can I do to better protect my organization?” We also dive into a recent variant of ransomware - “Locky” - and review case studies from Carbon Black customers that have stopped ransomware in its tracks.
A Brief History

History & Stats
Ransomware attacks date back to 1989 and have been the most pervasive cyber threat since 2005, with a dramatic spike in recent years. The resulting costs to targeted businesses are soaring. In fact, according to the 2018 Verizon Data Breach Investigations Report, ransomware has moved from the 22nd most common variety of malware in 2014 to the most common variety in 2018.

Two distinct varieties of ransomware have remained consistent in recent years: Crypto- and Locker-based. Crypto-ransomware variants encrypt files and folders, hard drives, etc. Locker-ransomware - most often seen with Android based ransomware - only locks users out of their devices.

New-age ransomware involves a combination of advanced distribution efforts, such as pre-built infrastructures used to easily and widely distribute new strains, as well as sophisticated development techniques, such as using crypters to ensure reverse-engineering. This combination requires advanced skills on the part of the attacker. But because the ROI is high, attackers are continually investing in these advanced forms of ransomware.

Offline encryption methods are also becoming popular. These attacks exploit legitimate system features, such as Microsoft’s CryptoAPI, eliminating the need for Command and Control (C2) communications.

Did You Know?
- 350+ variants of ransomware families have been identified
- Ransomware will attack a business every 14 seconds by the end of 2019
- This year, ransomware is one of the top 5 threats targeting the financial sector
- The U.S. receives 18.2 percent of all ransomware attacks.
- Ransomware attacks grow more than 350 percent every year.
The History Of Ransomware

1989-2015

AIDS Trojan
Infected 20k diskettes distributed at AIDS conference; symmetric cryptography; set in motion three decades of ransomware attacks

Unnamed Trojan
First ransomware to leverage mainstream adoption of anonymous payment services

CryptoLocker
First cryptographic malware spread by downloads from a compromised website and/or business professionals in the form of email attachments

CryptoWall
New and improved ransomware from creators of CryptoDefense; first to establish persistence by adding registry keys and copying itself to startup folders; netted $325 million for the threat actor

Koler
Considered first ‘Lockern worm’

SimpLLocker
First ‘crypto-based’ ransomware for Android devices that encrypted files on simply locked phones

TeslaCrypt
First ransomware to allow resiliency and persistence on victim machines

LowLevel04
First ransomware to be carried out manually by attackers by remoting into servers, mapping internal systems and drives before distributing ransomware; attackers were observed deleting application, security and system logs

CryptoDefense
Used Windows’ built-in encryption CryptoAPIs, 2048-bit RSA encryption & Tor/Bitcoin for anonymity

Sympa
First Android-based ransomware

CTB-Locker
First ransomware to communicate directly with a C2 server in Tor as well as delete Volume Shadow Copies on Windows machines

LockeRPin
First ransomware able to reset PIN on Android phones; $500 ransom to unlock phone

Chimera
First ‘dosing’ ransomware that threatened to publish sensitive or private files online

Archievus
First ransomware to use asymmetric encryption; encrypted everything in ‘My Documents’ and required users to make purchases from websites to obtain passwords to decrypt files

Reveton
Spawned ‘police-based’ ransomware including Urasy and Taily

| **ZCryptor** | One of the first ‘crypto-worms’ that self-propagates to infect external devices and other systems on the network, while also encrypting every machine and shared drive |
| **CyrptXXX** | Research suggests CyrptXXX is connected to the Reveton ransomware variant; typically observed after Bedep infections |
| **PowerWare** | A new instance of ransomware utilizing native tools, such as PowerShell on operating systems, discovered by CB Threat Research team in April, utilizes PowerShell, a core utility of current Windows systems, to do the dirty work, attempts to avoid writing new files to disk and tries to blend in with legitimate computer activity |
| **Jigsaw** | First to use Crypter to hide and encrypt source code of malware |
| **Maktub** | First to use ransom note containing characters from the movie series “Saw”; deleted files every 60 minutes if ransom not paid; resetting a machine resulted in 1,000 files being deleted |
| **Petya** | Delivered via Dropbox, overwrote Master Boot Record (MBR) of infected machines and encrypted physical drive; ransom doubled if payment not received in seven days |
| **SamSam (SAMAS)** | First to target JBoss servers and include a channel for attackers to communicate in real-time with victims via a .onion website |
| **7ev3n** | Demanded the highest ransom thus far, 13 bitcoins; first to date, to destroy Windows systems if ransom not paid |
| **Ransomware32** | First ransomware written in JavaScript, first to work on multiple OS including Linux, Windows and MacOS X |
| **Locky** | Spread via aggressive phishing campaigns and leveraged Dropper infrastructure; used to target hospitals in Kentucky, California and Kansas; started ransomware-in-healthcare trend |
| **KeRanger** | First MacOS X ransomware; signed with MAC development certificate allowing it to bypass Apple’s Gatekeeper security software |
| **7ev3n** | Demanded the highest ransom thus far, 13 bitcoins; first to date, to destroy Windows systems if ransom not paid |

---

The History of Ransomware

**2017-2019**

**WannaCry**
Cryptoworm that used NSA-leaked EternalBlue SMB exploit to infect 23,000 Windows endpoints in 150+ countries.

**SambaCry**
Continued the trend of using NSA tools to mine cryptocurrency and ransom machines running Linux.

**BadRabbit**
Redirected targets from legitimate sites to fake “Adobe Flash update” pages, where it then delivered the malware dropper delivered via “drive-by attack.”

**Reyptson**
First ransomware to conduct its own spam campaign directly from a victim’s configured Thunderbird email account.

**GandCrab**
Has had four significantly different versions since January 2018 and demonstrates how modern malware adjusts to the adapting cybersecurity environment.

**Ryuk**
Unlike common ransomware, Ryuk was used exclusively in tailored attacks. Its encryption was built for small-scale operations so that only crucial assets were infected, and therefore generally required a higher payment.

**NotPetya**
Cyber weapon disguised as Petya that used EternalBlue and Mimikatz to quickly spread from hijacked Ukrainian tax software.

**Leakerlocker**
Targeted Android devices without encrypting them. Instead, it threatened to send personal data (like texts and photos) to the user’s entire contact list.

**Adylkuzz**
Leveraged EternalBlue exploit, but focused on mining cryptocurrency instead of demanding ransom.

**LockerGoga**
Used Windows “living off the land” tools (LOLBins) to infect and encrypt machines.

**BadRabbit**
Redirected targets from legitimate sites to fake “Adobe Flash update” pages, where it then delivered the malware dropper delivered via “drive-by attack.”

**SambaCry**
Continued the trend of using NSA tools to mine cryptocurrency and ransom machines running Linux.

**Ryuk**
Unlike common ransomware, Ryuk was used exclusively in tailored attacks. Its encryption was built for small-scale operations so that only crucial assets were infected, and therefore generally required a higher payment.

**NotPetya**
Cyber weapon disguised as Petya that used EternalBlue and Mimikatz to quickly spread from hijacked Ukrainian tax software.

**Leakerlocker**
Targeted Android devices without encrypting them. Instead, it threatened to send personal data (like texts and photos) to the user’s entire contact list.

**Adylkuzz**
Leveraged EternalBlue exploit, but focused on mining cryptocurrency instead of demanding ransom.

**LockerGoga**
Used Windows “living off the land” tools (LOLBins) to infect and encrypt machines.

**BadRabbit**
Redirected targets from legitimate sites to fake “Adobe Flash update” pages, where it then delivered the malware dropper delivered via “drive-by attack.”

**SambaCry**
Continued the trend of using NSA tools to mine cryptocurrency and ransom machines running Linux.

**Ryuk**
Unlike common ransomware, Ryuk was used exclusively in tailored attacks. Its encryption was built for small-scale operations so that only crucial assets were infected, and therefore generally required a higher payment.

**NotPetya**
Cyber weapon disguised as Petya that used EternalBlue and Mimikatz to quickly spread from hijacked Ukrainian tax software.

**Leakerlocker**
Targeted Android devices without encrypting them. Instead, it threatened to send personal data (like texts and photos) to the user’s entire contact list.

**Adylkuzz**
Leveraged EternalBlue exploit, but focused on mining cryptocurrency instead of demanding ransom.

**LockerGoga**
Used Windows “living off the land” tools (LOLBins) to infect and encrypt machines.
RANSOMWARE IS NOW ESTIMATED TO BE A $8 BILLION CRIME

How Ransomware Works

Stages of an attack
Ransomware is similar to other malware in that it installs itself on a computer and runs in the background without the user's knowledge. But unlike malware that hides and steals valuable information, ransomware doesn't hide. As soon as ransomware has locked a user's machine and/or encrypted files, it notifies the user of its presence to make the ransom demand.

Here’s an example of the stages of a “locky” attack originating from a spear-phishing email

1. End user receives an email that appears to be from their boss. It contains a URL to a SaaS application such as Salesforce, Workday or ZenDesk.
2. The link opens a browser window and directs the user to a website that seems legitimate. It’s actually a landing page for an exploit kit hosted in a .cc .cc top level domain (TLD).
3. Upon loading the page, the web server hosting the exploit kit begins communicating with the victim machine. The server sends requests about versions of software such as Java to find a vulnerable version for which the kit has an exploit.
4. When a vulnerable version is confirmed, the kit attempts to exploit the vulnerability. Once successful, the exploit kit pushes down a malicious .EXE file – let’s call it “ransomware.exe.” The malicious binary on the victim machine then attempts to execute.
5. From this beachhead, the binary spawns child processes, including vssadmin .exe (shadow copy), to delete existing shadows on the victim machine and create new ones to hide in. The attacker does this to limit the possible recovery of files by the victim using Shadow Copies that Windows stores on a system.
6. NOTE: The inclusion of a child process containing Volume Shadow Copy processes is a behavior of a new Locky variant. A diagram and screenshots of this attack and how to detect it are provided in the section below, “Locky Variant - Shadow Copies.”
7. The binary also creates a PowerShell executable to propagate copies of itself throughout the filesystem. The executable also searches the filesystem for files of specific extensions and begins to encrypt those files.
8. The powershell .exe child process creates three copies of the originating malware binary, first in the AppData directory, next in the Start directory, and finally in the root C:\ directory. These copies are used in conjunction with the registry modifications to restart the malware upon reboot and login events.
9. After encrypting the victim’s files, the malware sends the encryption key and other host-specific information back to the command-and-control server.
10. The server then sends a message to the victim. This could be a simple “alert user of encryption and directions on paying us.” It could also include directions that result in downloading additional malware, which enables the attacker to steal credentials from the victim as well.

To amplify the victim’s distress, ransomware often includes a countdown clock with a deadline for paying the ransom - or else the decrypt key will be destroyed, eliminating any chance of recovery.

Paying the ransom often means the attacker will unlock the victim’s machine or provide the key to decrypt files. However, it rarely means the originating malicious binary, “ransomware.exe” in the case above, has been removed. That will require IT and SecOps support.

And the attack doesn’t necessarily end there. Attackers often load additional malware on a user’s machine, allowing them to harvest personal information, intellectual property, and credentials to sell for additional revenue.
Ransomware

Attack Anatomy

**PHASE 1**
- Attacker Sends Spam Email
- Hits User’s Inbox
- Bypasses Victim's Spam Filter

**MALWARE XYZ.exe** is delivered, launches legitimate child processes cmd.exe, PowerShell, VSSadmin + encryption mechanism

**PHASE 2**
- User clicks on malicious link
- Antivirus Fails

**C:\**
- Adds registry entry to run and runonce
- Copies malware to [AppData, Startup, C:]

**PHASE 3**
- Encryption
- Encrypts Files on victim mounted drives
- Connects with attacker’s C&C server to deliver info / get instructions
- Attacker attempts to move laterally across the enterprise

Ransom Note Delivered
GUIDE: ADVANCE YOUR RANSOMWARE DEFENSES

Locky Variant –Shadow Copies

Defeating Locky and Volume Shadow Copies

Ransomware is becoming increasingly sophisticated. Comparing today’s ransomware to yesterday’s malware is like comparing a computer to an abacus. One advanced example is “Locky,” a CryptoLocker variant that deletes all “Volume Shadow Copies” to prevent restoring from backup, and then encrypts the files for ransom. This can be a terrible - and expensive - headache for unprepared IT and security teams.

Shadow Copy is a Microsoft Windows technology that allows the capture of backup copies (snapshots) of computer files or volumes. Backups can be taken even when the files are in use. It’s implemented as a Windows service called the “Volume Shadow Copy Service.” Shadow copies can be created on local and external volumes by any Windows component that utilizes it, such as when creating a scheduled Windows backup or automatic system restore point.

Carbon Black has observed various ransomware techniques utilizing volume shadows. Lately, it's been used for avoiding detection and for anti-analysis.

A specific attack we've seen consists of the following steps:

- Attackers drop malware on the filesystem via whatever infection mechanism they choose
- Create a volume shadow
- “Mount” the shadow and execute the malware
- Unmount the shadow and delete it

What’s unique about this technique is that even after unmounting and deleting the shadow, the executed malware will still run. On Windows XP, the vssadmin tool isn’t able to create persistent shadows. Starting with the Windows Vista SDK, Microsoft supplied a binary called Vshadow to allow this.

GUIDE: ADVANCE YOUR RANSOMWARE DEFENSES
GUIDE: ADVANCE YOUR RANSOMWARE DEFENSES

The malware is placed at the root of the shadow after it was created. A directory listing of C:\Windows\System32\msdc reveals the malware on the normal filesystem but living inside the shadow filesystem. Once the symlink has been created the contents of the shadow are accessible via normal filesystem operations like the directory listing seen above.

Once the file system setup is in place, the malware is started just like any other executable.

When the malware is started and shown in a tool like process explorer it shows that it is running from C:\Windows\System32\msdc.

At first glance, that path doesn’t look too suspicious.

Once the malware is started, the attackers can unmount and delete the shadow and the malware continues to run.

To remove as much forensic evidence as possible, the attacker would unmount the directory and delete the shadow with vssadmin.

This technique is an effective hiding mechanism that throws in a little anti-forensics, demonstrating how ransomware is evolving.

Ransomware can be dangerously effective. Recent additions of features such as removing shadow copies makes it even more dangerous. Visibility is a key requirement for detecting and preventing such ransomware.
Advance Your Ransomware Defenses

Stop Ransomware Before It Starts with CB Predictive Security Cloud

Even the most educated end users, well versed in security best practices such as never clicking on email attachments, can become victims of drive-bys and other sophisticated exploit kits that can deliver ransomware. Traditional, signature-based antivirus can sometimes protect an organization’s endpoints from existing, known malware. However, there are new variants of ransomware, such as Locky, as well as advanced attacks that leverage PowerShell, scripts, macros, remote shell attacks and memory-based attacks that AV simply cannot stop. These attacks now make up more than 50 percent of the attacks targeting enterprise organizations. The first step every organization can take is to stop relying on traditional, signature-based AV solutions to defend their endpoints, servers and critical systems.

Carbon Black offers a powerful next-generation antivirus (NGAV) and endpoint detection & response (EDR) solution delivered through Carbon Black’s delivered through the CB Predictive Security Cloud (PSC). Using Carbon Black’s breakthrough streaming analytics, the PSC can stop malware and non-malware attacks, using deep analytics to inspect files, connect the dots between events, and identify malicious behavior. This comprehensive approach blocks traditional malware as well as increasingly common malware-less attacks that exploit memory and scripting languages such as PowerShell.

Detect Advanced Ransomware Event Streams

The PSC stops ransomware attacks, including the Locky variant explained earlier in this eBook, more effectively and efficiently than other solutions might. And it does so at multiple points in the infection workflow for layered defense.

Ransomware itself has evolved in recent years to incorporate some of its own unique behaviors that make its encryption and extortion efforts more effective. To combat this, the PSC employs a number of innovative techniques to prevent and disrupt them. To prevent ransomware from destroying backups, a new ransomware technique designed to increase the likelihood of a payout, the PSC monitors access and modification attempts to shadow copies and master boot records. In addition, the PSC uses “canary files,” benign files that sit on the endpoint, as well as other file heuristics to lure evasive and stealthy ransomware variants into a trap that exposes them, allowing active prevention to take over.

Once ransomware is blocked, the PSC provides full visibility into how the attack happened. By capturing and analyzing behavior in advance, the PSC pinpoints the exploit. Armed with this insight from the PSC, IT and SecOps teams can proactively patch the vulnerabilities exploited by the exploit kit. the PSC also provides a suite of remediation tools to quarantine machines, blacklist software, and remove unwanted items. the PSC uses a lightweight sensor that installs seamlessly and consumes less than one percent of the CPU, disk, and network. Once installed, the PSC can be completely managed from the cloud through an easy-to-use web-based interface.

Block Ransomware Even If It’s Never Been Seen Before

What makes this approach especially powerful is the fact that it catches ransomware before reputation ever needs to be checked. This means that even if the endpoint is offline and unable to check cloud-based reputation, the stream of events would be detected and automatically blocked by the the PSC sensor. However, when connected the PSC checks the reputation of all executables and binaries downloaded to an endpoint against the CB Predictive Security Cloud. The CB Predictive Security Cloud contains reputation scores on more than 8 billion files, adding approximately 200,000 per day, while also leveraging threat intelligence from more than 20 threat partners to determine good software and binaries from malicious.

Once ransomware is blocked, the PSC monitors access and modification attempts to shadow copies and master boot records. In addition, the PSC uses “canary files,” benign files that sit on the endpoint, as well as other file heuristics to lure evasive and stealthy ransomware variants into a trap that exposes them, allowing active prevention to take over.

If the XYZ.exe is a zero-day and has no reputation score on file, the PSC would block the execution of the malicious binary based on behavior. In this example, the PSC would recognize the attempt on behalf of the executable to inject code into legitimate running processes or the creation of new child processes from packed memory buffers. the PSC is able to detect this infection workflow in part because of its focus on patterns of attack versus simply indicators of compromise. Additionally, in this scenario, the PSC would also block the attempt of the executable to ‘phone home’ to the C&C server.

FIGURE 5
Ransomware Defense Cheat Sheet

Defense in Depth: 14 Keys to Protecting Against Ransomware

Ransomware infections can be devastating and recovery efforts threaten to financially cripple an organization. Prevention is the most effective defense. Deploying a next-generation endpoint security product like Carbon Black that can detect and stop ransomware attacks is an obvious first step. Here are 14 additional best practices recommended by the U.S. government and other experts to combat ransomware:

1. **Back up data regularly.** Verify the integrity of those backups and test the restoration process to ensure it’s working.

2. **Secure your offline backups.** Backups are essential: if you’re infected, a backup may be the only way to recover your data. Ensure backups are not connected permanently to the computers and networks they are backing up.

3. **Configure firewalls to block access to known malicious IP addresses.**

4. **Logically separate networks.** This will help prevent the spread of malware if every user and server is on the same network newer variants can spread.

5. **Patch operating systems, software, and firmware on devices.** Consider using a centralized patch-management system.

6. **Implement an awareness and training program.** End users are targets, so everyone in your organization needs to be aware of the threat of ransomware and how it’s delivered.

7. **Scan all incoming and outgoing emails** to detect threats and filter executable files from reaching end users.

8. **Enable strong spam filters to prevent phishing emails** from reaching end users and authenticate inbound email using technologies such as Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent spoofing.

9. **Block ads.** Ransomware is often distributed through malicious ads served when visiting certain sites. Blocking ads or preventing users from accessing certain sites can reduce that risk.

10. **Use the principle of “least privilege” to manage accounts.** No users should be assigned administrative access unless absolutely needed. If a user only needs to read specific files, the user should not have write access to them.

11. **Leverage next-generation antivirus technology** to inspect files and identify malicious behavior to block malware and malware-less attacks that exploit memory and scripting languages like PowerShell.

12. **Use application whitelisting,** which only allows systems to execute programs known and permitted by security policy.

13. **Categorize data based on organizational value** and implement physical and logical separation of networks and data for different organizational units.

14. **Conduct an annual penetration test** and vulnerability assessment.
Next Generation Ransomware Prevention

Ransomware is here, and it’s not going away. Criminals are making money at an alarming rate with little resistance. There have been more ransomware variants in the last 18 months than all of the 29 previous years. By using ransomware, cyber criminals have had a free run at organizations’ critical data. It’s time to stem the tide, now.

In addition, ransomware variants are implementing new, innovative techniques that employ unknown binaries and non-malware tactics to evade and bypass traditional defenses. Their encryption techniques go beyond simple files and shares to make it even harder to restore using backups and their targets are increasingly becoming organizations with much more to lose (and more money to payout) than individuals.

Stopping ransomware requires a defense-in-depth approach; there is no silver bullet to security. Software alone is not the answer. IT and SecOps teams must build a strategy that combines user training, next-generation endpoint security, and backup operations.

Every strategy should start with the simplest, most immediate risk-mitigation techniques available in order to limit the attack surface, such as next-generation antivirus and strong spam filtering. Concurrently, user training and backup infrastructures should be evaluated, implemented, and practiced.

The PSC provides the most effective and easy-to-use next-generation antivirus solutions available - proven to stop ransomware variants, such as “Locky.”

To learn more about the PSC, register for a private solution demonstration, or speak with a CB Solution Architect, visit: carbonblack.com/ransomware

Case Study: Financial Services

Taking Preemptive Action Against Ransomware

A well-known financial services company needed to protect its servers and workstations from emerging attacks, especially ransomware. Once they realized that traditional antivirus was unsuited for the job, they found the PSC was able to give them the insight and protection they need.

Here’s an example of the stages of a “locky” attack originating from a spear-phishing email

1. **GETTING AHEAD OF THE RANSOMWARE THREAT** As new instances of ransomware began popping up throughout their company’s environment, it became apparent that a new solution was needed to protect endpoints. Though the instances were isolated, those employees that were affected saw considerable downtime, which impacted their ability to do their jobs.

2. **THE SEARCH FOR A MORE EFFECTIVE PLATFORM** The security team recognized that a small problem today would quickly escalate out of their control if not properly managed. The first step was an internal review of existing security platforms to see if they could be tuned or reconfigured to combat this growing threat. They soon realized that what they had, including their traditional antivirus platform, was just not effective. This initiated an extended search to look into next-generation platforms that could stand up to unknown and evasive variants.

3. **INSIGHT AND ADVANCED PREVENTION ARE ESSENTIAL**

   The security team realized there were two requirements if they were going to effectively combat ransomware - increased insight into advanced techniques, and a powerful prevention engine that could keep threats at bay. The PSC proved to be the only platform that could meet both requirements. Because ransomware is constantly evolving, signature-based approaches cannot stop them from infecting machines and causing damage.

4. **ADDED BENEFITS: VISIBILITY INTO ENDPOINT ACTIVITIES**

   An added benefit with the PSC is more visibility into endpoint activities and behavior. The PSC can provide process-level visibility at the endpoint, offering an extended view that helped them understand where potential threats were forming before they were able to execute.

Cloud-delivered Endpoint Security

The CB Predictive Security Cloud is a cloud native endpoint protection platform (EPP) that consolidates security and provides you with what you need to secure your endpoints, using a single lightweight agent.

Conclusion
Carbon Black (NASDAQ: CBLK) is a leader in cloud endpoint protection dedicated to keeping the world safe from cyberattacks. The CB Predictive Security Cloud® (PSC) consolidates endpoint security and IT operations into an endpoint protection platform (EPP) that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks.

More than 5,300 global customers, including 35 of the Fortune 100, trust Carbon Black to protect their organizations from cyberattacks. The company’s partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world’s leading IR firms, who use Carbon Black’s technology in more than 500 breach investigations per year.

Carbon Black and CB Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and/or other jurisdictions.