FEATURE

4 types of ransomware and a timeline of attack examples

There are four main types of ransomware, but many examples of ransomware strains. Learn how the ransomware types work, and review notable ransomware attacks and variants.

Isabella Harford, Assistant Site Editor
Ashwin Krishnan, Mobilematics

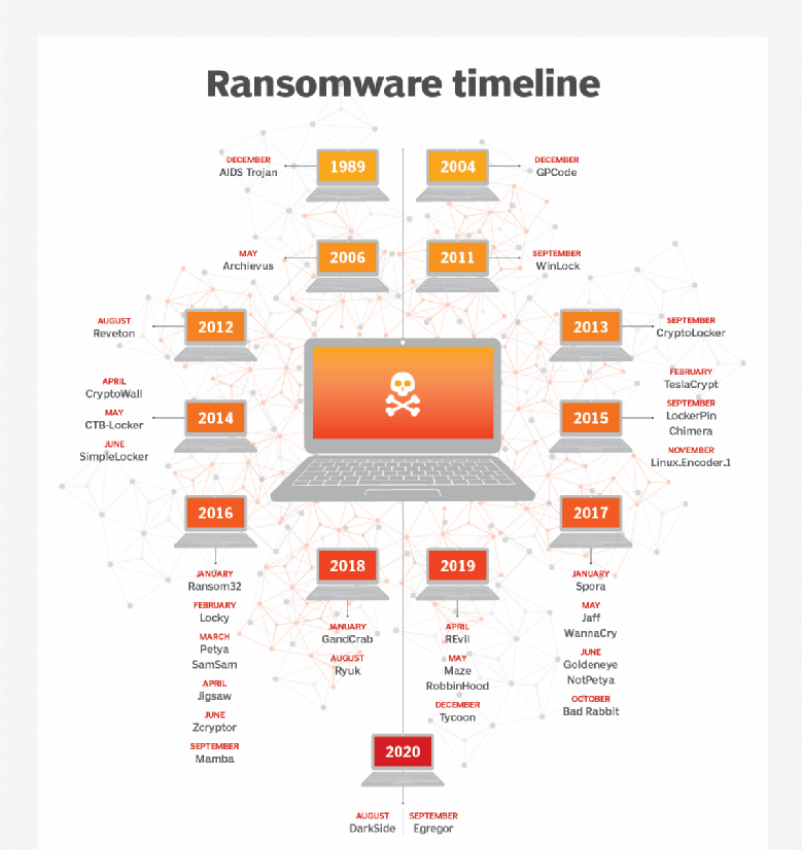
Ransomware is one of the most effective strategies for attacking businesses, critical infrastructures and individuals. This type of malware infects computers and prohibits or severely restricts users or external software from accessing devices or entire systems until ransom demands have been met.

To understand the concept, let's look at the four types of ransomware, along with examples of specific ransomware strains and their effect on the security landscape.

4 types of ransomware

Historically, the two main types of ransomware are crypto and locker. More recently, double extortion and ransomware as a service (RaaS) have become popular among threat actors.

1. **Locker ransomware** blocks access to computer systems entirely. This variant uses social engineering techniques and compromised credentials to infiltrate systems. Once inside, threat actors block users from accessing the system until a ransom is paid. A pop-up on the victim's screen may appear saying, "Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine," or "Your computer has been infected with a virus. Click here to resolve the issue."
2. **Crypto ransomware** is more common and widespread than locker ransomware. It encrypts all or some files on a computer and demands a ransom from the victim in exchange for a decryption key. Some newer variants also infect shared, networked and cloud drives. Crypto ransomware spreads through various means, including malicious emails, websites and downloads.
3. **Double extortion ransomware** encrypts files and exports data to blackmail victims into paying a ransom. With double extortion ransomware, attackers threaten to publish stolen datathreaten to publish stolen data if their demands are not met. This means that, even if a victim can restore their data from backup, the attacker still has power over them. However, paying the ransom does not guarantee protection of the data either, as the attackers have access to the stolen data.
4. **RaaS** involves perpetrators renting access to a ransomware strain from the ransomware author, who offers it as a pay-for-use service. RaaS creators host their ransomware on dark net sites and allow criminals to purchase it as a subscription -- much like a SaaS model. The fees depend on the ransomware's complexity and features, and generally, there's an entry fee to become a member. Once members infect computers and collect ransom payments, a portion of the ransom is paid to the RaaS creator under previously agreed-upon terms.



History of ransomware

Examples of ransomware strains

Ransomware isn't anything new, but it remains a major challenge for individuals, companies, governments and organizations. Take a look at some of the most notable examples of ransomware from the past 30-plus years here.

THIS ARTICLE IS PART OF

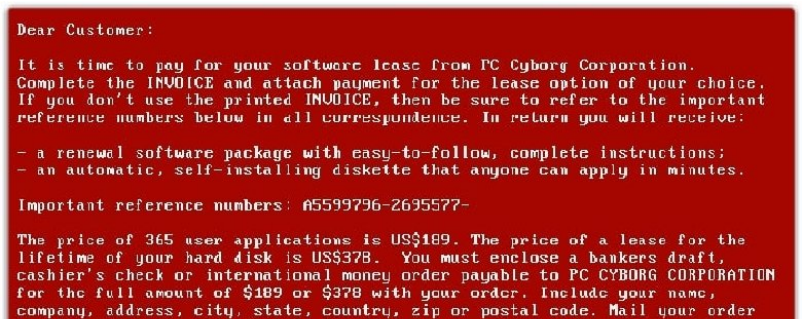
The complete guide to ransomware

Which also includes:

- How to create a ransomware incident response plan
- ransomware
- How to prepare for ransomware and phishing attacks

December 1989: AIDS Trojan

The first documented ransomware was created by Joseph Popp, a Harvard-educated biologist. Popp mailed 20,000 floppy disks containing the AIDS Trojan, also known as the PC Cyborg virus, to researchers across the globe. Recipients were led to believe the disks contained Popp's AIDS research, but once opened, victims' files were encrypted with simple symmetric cryptography. Victims were told to send $189 to a P.O. box in Panama to regain access. Popp, whose motives remain a mystery, has been credited as the founder of ransomware.



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2635577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
```

Popp's ransom note with the AIDS Trojan demanded users send $189 to a P.O. box in Panama.

December 2004: GPCode

After a 15-year lull, GPCode marked the beginning of the internet era for ransomware. The malware, spread via email, encrypted victims' files and renamed them *Vnimanie*, meaning *attention* in Russian. Unlike many of today's ransomware attacks, GPCode's authors focused on volume rather than individual payouts, sending an exorbitant number of malicious emails and demanding $20 to $70 ransoms.

May 2006: Archievus

Archievus was the first ransomware to use a 1,024-bit Rivest-Shamir-Adleman (RSA) encryption key. It targeted Windows systems and spread via malicious URLs and spam emails. The malware targeted computers' "My Documents" folders. Once folders were encrypted, victims were directed to an online store; only after victims made a purchase would they receive a password to unlock their files. While the RSA encryption key was difficult to crack, Archievus was quickly abandoned once it was discovered the attackers used the same password to lock all files.

September 2011: WinLock

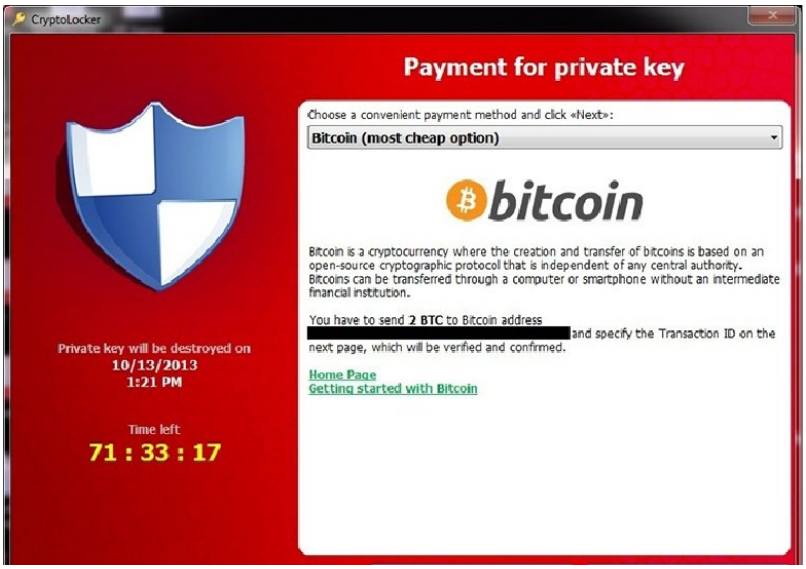
WinLock was the first locker ransomware to hit the headlines. The nonencrypting ransomware infected users via a malicious website. Victims were instructed to purchase a $10 text message code. After inputting the code into their devices, victims were prompted to call a supposed toll-free number. The calls, however, were rerouted, and the victims incurred additional fees.

August 2012: Reveton

Reveton was a form of financial ransomware delivered via drive-by-download attacks. Once infected, a pop-up alert purported to be from law enforcement claimed the victim committed a crime -- such as downloading pirated software -- and threatened imprisonment if the "fine" was not paid via a money payment service. Later variants used victims' webcams, requested bitcoin payments, distributed password-stealing malware, and infected Mac and mobile OSes.

September 2013: CryptoLocker

CryptoLocker is one of the first examples of sophisticated ransomware. It locked users out of their devices and then used a 2,048-bit RSA key pair to encrypt systems and any connected drives and synced cloud services. This increased the chances of payment because, even if the victim removed the lock, access would not be restored as the system was encrypted. CryptoLocker spread via malicious attachments in spam FedEx and UPS tracking notices, as well as infected websites. Attackers requested a $300 ransom to unlock devices. The ransomware reportedly earned $27 million in ransom payments in its first two months.



CryptoLocker ransom note requested users pay 2 bitcoin to unlock their devices.

April 2014: CryptoWall

Dell Secureworks Counter Threat Unit called CryptoLocker copycat CryptoWall "the largest and most destructive ransomware threat on the internet" in August 2014. However, the ransomware never became as well known as its predecessor. In the strain's first six months, it infected 635,000 systems and earned more than $1.1 million in ransom payments. CryptoWall spread via phishing emails and malicious advertisements on legitimate websites. In many instances, victims could have avoided the attack if they simply updated their software and backed up their servers.

May 2014: CTB-Locker

Curve-Tor-Bitcoin Locker used elliptic curve cryptography to encrypt victims' files and the Tor browser to obfuscate its communications activities. Once infected via malicious emails and downloads, victims were prompted to pay a ransom via bitcoin. CTB-Locker was one of the first ransomware strains to use multilingual notices to inform victims of infection. It also marked the start of the widespread use of cryptocurrency for ransom payments.

June 2014: SimpleLocker

SimpleLocker, sometimes referred to as Simplocker, was the first ransomware to target Android devices. The Trojan scanned SD cards and then encrypted images, documents and videos. Later versions could access victims' cameras. It was known for collecting devices' numbers, model numbers and manufacturers. Like CTB-Locker, SimpleLocker used Tor to prevent being traced. Attackers demanded a ransom in exchange for a password to regain access.

February 2015: TeslaCrypt

TeslaCrypt got its start targeting computer gamers. Its first iteration could only encrypt files smaller than 268 MB. Attackers demanded $500 in ransom and threatened to double the fee if victims delayed paying. In 2016, the cyber gang behind TeslaCrypt released a master key, which enabled victims to

LockerPin was the first PIN-locking mobile ransomware to target Android OS devices. It infected users after being downloaded from third-party app stores. Unlike its SimpleLocker predecessor, which was the first to encrypt files on mobile devices, LockerPin could override administrative privileges, stop antivirus programs running on the device and change the victim's PIN. Even if the $500 ransom was paid, however, attackers were unable unlock victims' devices as the PINs were randomly generated and unknown to the attackers.

September 2015: Chimera

The Chimera ransomware was one of the first strains that threatened to leak victims' data if a 2.5 bitcoin ransom was not paid. It remains unclear, however, if attackers ever stole the files' data or if they were idle threats. Chimera spread via emails containing malicious Dropbox links. In July 2016, rival ransomware group Petya released 3,500 Chimera decryption keys. Other Chimera decryptors are also available.

November 2015: Linux.Encoder.1

Linux.Encoder.1 was the first ransomware Trojan to target Linux-based machines. After exploiting a flaw in the e-commerce Magento platform, the Trojan encrypted MySQL, Apache, and home and root folders. Attackers demanded a single bitcoin in exchange for the decryption key. Patching systems against the Magento flaw prevented users from falling victim.

January 2016: Ransom32

Ransom32 was the first JavaScript ransomware. This made it a cross-platform, "write once, infect all" ransomware, able to infect Windows, Linux and Mac OSes.

February 2016: Locky

Locky ransomware used the Necurs botnet to send phishing emails with Word or Excel attachments containing malicious macros. It encrypted files on Windows OSes. A June 2016 version could detect if the malware was being run in a sandbox, and a July 2016 variant could encrypt files offline. Locky resurfaced in September 2017 in an attack where 23 million phishing messages were sent in a 24-hour window.

March 2016: Petya

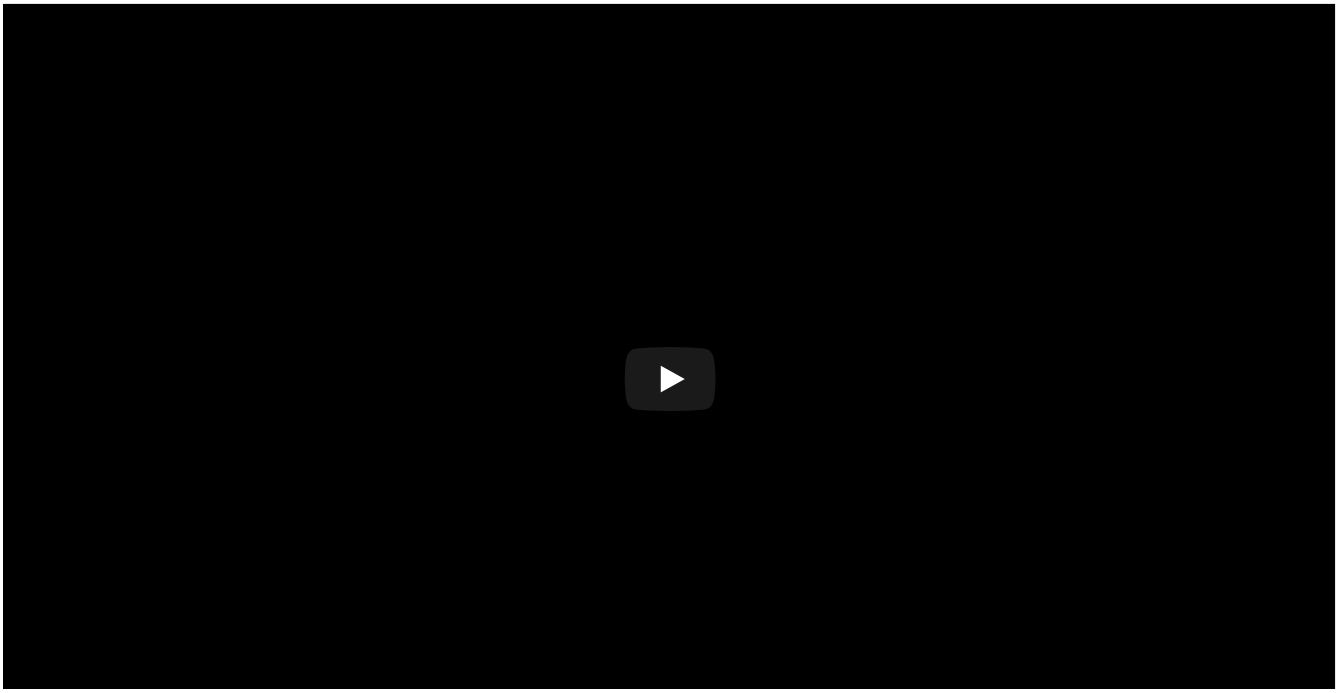
Petya was labeled the "next step in ransomware evolution" by Check Point researchers due to its ability to overwrite the master boot record (MBR) and encrypt the master file table (MFT), which logs the metadata and the physical and directory location of all files on a device. These three steps locked victims out of their system. Petya infected Windows-based systems through phishing emails.

March 2016: SamSam

SamSam is notable for its manual operations. After identifying their victims, attackers use brute-force and legitimate Windows tools to infect specific devices. After executing the ransomware, a bitcoin ransom is demanded. Later versions incorporated additional complexity, encryption and obfuscation techniques. Targets and victims included healthcare, education and critical infrastructure. SamSam was used in the 2018 attacks against the city of Atlanta and the Colorado Department of Transportation. A 2018 Sophos report found the ransomware brought in $6 million since its creation.

April 2016: Jigsaw

Victims of the Jigsaw ransomware, which infected systems via malicious emails, were confronted by a photo of Billy, the puppet from the *Saw* film franchise, and a countdown timer. If the $150 ransom wasn't paid in an hour, one of the victim's files was deleted. Each hour that went by, the number of files deleted increased. If victims attempted to restart their devices, up to 1,000 files were instantly deleted. A decryption key has since been released.



[redacted]

June 2016: Zcryptor

Zcryptor was one of the first cryptoworms, a hybrid computer worm and ransomware. It self-duplicated to copy itself onto external connected devices and networks. Zcryptor encrypted files until a ransom of 1.2 bitcoin was paid to the attackers; after four days, the ransom increased to 5 bitcoin.

September 2016: Mamba

Mamba, also known as HDDCryptor, was a disk-encrypting ransomware that spread using a legitimate DiskCryptor encryption tool. It was notably used in an attack on the San Francisco Municipal Transportation Agency. When railway passengers tried to purchase tickets, a message appeared on the screen notifying them of the attack. Reports have suggested Mamba exploited an unpatched Oracle server program; a simple system update could have prevented the attack.

January 2017: Spora

Spora, named after the Russian word for *spore*, is notable for its ability to work offline and its sophisticated payment system. It spread through phishing emails containing malicious zip attachments. Once downloaded, Spora encrypts files using a combination of Advanced Encryption Standard and RSA algorithms. Spora's offline component enables the malware to distribute without generating traffic to other online servers in the network. In August 2017, an upgraded Spora was released that enabled attackers to steal browsing information and record keystrokes.

May 2017: Jaff

Jaff was detected a day before the infamous WannaCry attack. While it mimicked Locky, it was far less sophisticated. Jaff used the Necurs botnet to spread roughly 5 million malicious emails per hour. Attackers demanded $3,300 in bitcoin -- a much higher ransom than other variants.

May 2017: WannaCry/WannaCrypt

WannaCry was used during the May 2017 global cyber attack against systems in 150 countries. In May 2019, it was reported the ransomware spread to nearly 5 million vulnerable devices. The self-replicating cryptoworm affected high-profile organizations, including the U.K.'s National Health Service, FedEx, Honda and Boeing. Also known as WannaCrypt, WannaCryptor and Wanna Decryptor, it spread via the National Security Agency-leaked EternalBlue exploit, a vulnerability in legacy versions of Server Message Block. Microsoft had released a patch in March 2017, but it was not widely updated. As a worm, it self-replicated to infect. WannaCry was touted as the biggest ransomware attack to date in 2017.

June 2017: Goldeneye

Goldeneye, a variant of Petya, is often called WannaCry's sibling. It spread via phishing and encrypted individual files, the MBR and the MFT. It also propagated via EternalBlue. Infected devices crashed, restarted and then displayed a ransom pop-up screen. A decryptor became available the next month.

June 2017: NotPetya

The Petya variant dubbed NotPetya is considered ransomware, but as a wiper, it focuses on destroying files rather than collecting money. Like Petya, it encrypts the MBR and MFT. Unlike Petya, after encryption, it destroys the device's content. Even if victims pay the ransom, they never get their files back. NotPetya uses multiple attack vectors, including legitimate software tools.

October 2017: Bad Rabbit

Bad Rabbit, a variant of NotPetya, uses fake Adobe Flash installer advertisements to target victims. Like Petya, Bad Rabbit exploits EternalBlue and encrypts the MBR. Once a device is infected, a message appears demanding 0.05 bitcoin. If victims don't pay within 40 hours, the ransom increases.

January 2018: GandCrab

GandCrab was the first RaaS variant to demand payments in Dash cryptocurrency. It used a .bit top-level domain, which is not sanctioned by the Internet Corporation for Assigned Names and Numbers, to ensure secrecy. GandCrab spread through emails, exploit kits and other malware campaigns. It was responsible for more than 50% of the ransomware market by August 2018. In 2019, the ransomware gang behind GandCrab retired and released a decryption tool.

August 2018: Ryuk

Ryuk, named after a manga character, was one of the first variants to encrypt network drives, delete shadow copies and disable Windows System Restore, making it impossible for victims to recover without external backups or rollback technology. Ryuk is distributed by phishing emails containing malicious Microsoft Office documents. It was used in an attack against Tribune Publishing Company in December 2018. In 2019 and 2020, it was used in several attacks against healthcare organizations. Targets and victims also include governments, school systems, and other public and private sector companies.

April 2019: REvil

REvil, also known as Sodin and Sodinokibi, may be related to 2018's GandCrab. The two strains have striking similarities and were deployed together on victims' systems in early attacks, before GandCrab's retirement. Early attacks exploited an Oracle WebLogic vulnerability and a Windows zero-day vulnerability. Later exploits infiltrated systems through phishing, Remote Desktop Protocol (RDP) flaws, VPN attacks and supply chain attacks. It uses double extortion and has a dark web leak site, known as the Happy Blog. REvil was used in the notable attacks against Acer, JBS USA and Kaseya. The ransomware group went offline in July 2021 but reemerged in September 2021. A universal decryptor was released in September 2021 for victims of attacks pre-July 13, 2021.

May 2019: Maze

Maze, a variant of ChaCha, spread via spam emails, RDP attacks and exploit kits. It is one of the first examples of double extortion ransomware. In June 2019, Maze announced the creation of a cartel of cybercrime gangs. Maze shuttered operations in November 2020.

May 2019: RobbinHood

RobbinHood infiltrates victims' networks through phishing schemes, RDP attacks or other Trojans, sometimes abusing CVE-2018-19320, a Gigabyte kernel driver vulnerability. It disables services and protective programs, disconnects network shares, deletes shadow copies, clears event lots and disables Windows automatic repair. RobbinHood's ransom demands range from 3 to 13 bitcoin. The ransomware strain was notably used in attacks against the cities of Baltimore and Greenville, N.C., neither of which paid the ransom. The city of Baltimore reportedly paid $18 million in recovery costs, as opposed to a $114,000 ransom.

December 2019: Tycoon

Tycoon targets Windows and Linux environments at educational institutions and software companies. BlackBerry researchers said it is the first ransomware strain to use the Java image, or JIMAGE, format to create and deliver a customized malicious Java Runtime Environment build. Once inside a network, Tycoon disables antimalware programs and can remain hidden for months before encrypting file servers and demanding a ransom. A decryptor key was posted online, which decrypts some, but not all, affected systems.

August 2020: DarkSide

DarkSide, the malware used in the Colonial Pipeline attack in May, is a RaaS that targets high-profile victims. It uses double extortion, command and control via Tor, and advanced obfuscation techniques, among other stealth tactics. In May 2021, the ransomware gang announced its operations were suspending following pressure from the U.S. government. BlackMatter, a ransomware group that emerged in July 2021, has noted similarities to the DarkSide and REvil gangs.

September 2020: Egregor

Egregor, a variant of the Sekhmet ransomware, is a RaaS that many speculate to be former Maze affiliates. It was used in attacks against Barnes & Noble and Kmart, among others. Egregor is a double extortion strain and publicly shames its victims. Once the ransom is paid, the attackers decrypt the victims' systems and offer victims advice on how the company can better protect its network and avoid future attacks. An undisclosed number of Egregor affiliates were arrested in February 2021. Around the same time, the ransomware gang's infrastructure went offline.

This was last published in October 2021

Dig Deeper on Emerging cyberattacks and threats

The history and evolution of ransomware

By: Isabella Harford

ransomware as a service (RaaS)

By: Sean Kerner

Malware vs. ransomware: What's the difference?

By: Andy Patrizio

ransomware

By: Alexander Gillis

SearchCloudSecurity

Evaluate cloud database security controls, best practices

If your company is using a cloud database provider, it's critical to stay on top of security. Review the security features ...

All about cloud-native application protection platforms

The cloud-native application protection platform, or CNAPP, is the latest in a slew of cloud security acronyms. Learn what it is ...