PREVEIL

Cybersecurity and Ransomware Protection for Colleges and Universities

Executive Summary

THE ALARMING PACE of cyber and ransomware attacks has attracted attention at the nation's highest levels and throughout our public and private sectors. Prominent examples abound. In 2021, the Colonial Pipeline attack by an Eastern European group in May exposed the remarkable vulnerability of US infrastructure. The Kaseya software attack by the Russia-based group REvil in July affected some 1,500 companies in 17 countries. Closer to home, ransomware attacks on colleges and universities doubled since the onset of the pandemic, as cybercriminals have exploited institutions' vast attack surfaces and targeted the wide array of valuable research and personal data they collect. Known cases represent a range of institutions, from the University of California, San Francisco School of Medicine to Central Piedmont Community College.[1] The surge in attacks led to an **FBI advisory** specifically for higher education institutions, outlining attack methods and recommended preventative actions.

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

Despite the increasing sophistication and frequency of attacks, universities, businesses, cities, and other potential ransomware victims need not feel defenseless. Today, tools that offer military grade cybersecurity are readily available beyond the defense industry.

PreVeil's file sharing platform, for example, provides world class security but is simple to deploy, easy to use, and affordable for any size college or university. Hundreds of defense contractors use PreVeil to protect critical data, but so do law firms, financial firms, and universities. If your institution is shut down by a ransomware attack, the most recent uncorrupted versions of your data can be readily recovered because PreVeil retains every version of all your data on an entirely separate system. You won't have to pay a ransom to stay in operation.

If your institution is shut down by a ransomware attack, the most recent uncorrupted versions of your data can be readily recovered because PreVeil retains every version of all your data on an entirely separate system.

PreVeil was built from the ground up to make world class security accessible and affordable. We believe that if security isn't simple to use, it won't be used. PreVeil's simple design helps you protect what matters most—your data and files, emails, finances, and reputation—and keeps your institution running smoothly.

[1] *Colleges a 'Juicy Target' for Cyberextortion*, Inside Higher Ed, March 19, 2021.

CISA *Ransomware Guide*: Best Practices

Ransomware attacks are increasing for several reasons. One critical enabler is the growth of cryptocurrency, which is extremely difficult to trace and has made it easy for cybercriminals to collect ransoms. At the same time, cybercriminals have adopted corporate practices, with specialization and distributed responsibilities to form an efficient production line of organized cybercrime. REvil, for example, develops ransomware and its affiliates execute attack campaigns and negotiate and collect the ransoms, even setting up help desks to assist victims with purchasing Bitcoins. Finally, cybercriminals have found safe havens, such as Russia, that allow them to operate with impunity.

In response to these trends and the rapid increases in ransomware attacks and payoff demands that they fuel,[2] CISA (the Cybersecurity and Infrastructure Security Agency) teamed up with MS-ISAC (the Multi-State Information Sharing & Analysis Center) to publish a ***Ransomware Guide*** in 2020. The guide offers several best practices for preventing or minimizing the effects of ransomware attacks.

The guide's paramount best practice is to *maintain offline, encrypted backups of data*. The experts explain that maintaining offline, current backups is their top recommendation simply because there is no need to pay a ransom for data that is readily accessible to your organization.

PreVeil's file sharing platform encrypts and retains every version of all your data in Amazon's cloud—and backs that up, too, in a separate facility in

HOW IT WORKS: PREVEIL'S MULTIPLE LAYERS OF DATA PROTECTION

PreVeil constantly backs up, encrypts, and retains every version of all your data and files. This is done via an append-only technique, which makes previously saved versions of documents immutable; that is, they are unchangeable. Only changes made since the most recent backup can be saved (i.e., appended) to a document to create its new, most up-to-date version. If that most up-to-date version has been corrupted by ransomware and then backed-up, PreVeil can readily recover the immediate prior version of your document, which cannot have been corrupted given the append-only technique.

CISA warns that some ransomware is able to delete backup systems. That's a far higher risk if you use in-house backup systems, where a single attack can compromise all data, including backups. With PreVeil's Amazon cloud backup, on the other hand, the cybercriminals would need to carry out two entirely separate attacks—one on your institution's network and another on PreVeil's. The key point is that your institution's vulnerabilities do not transfer to PreVeil.

In addition to constantly encrypting all your data and saving every version in an immutable format, PreVeil also replicates your encrypted data from Amazon cloud to another, geographically-distant area of the country, so that your data can be recovered even in the event of a large-scale disaster. PreVeil's backup of its backup is done every 24 hours—again, using world class security to do so.

[2] From 2018 to 2020, ransomware attacks increased nearly tenfold. See: https://www.bitsight.com/blog/kaseya-ransomware-attack

a different location. (See related sidebar.) This means that if your institution is shut down by a ransomware attack, PreVeil can readily recover the most recent uncorrupted versions of all your files, correspondence and data.

Additional best practices in the guide address a wide range of concerns including, for example, the use of passwords (or not), principles of least privilege, and centralized log and event management and analysis.

The remainder of this brief describes how PreVeil helps you implement critical best practices for preventing or minimizing the effects of ransomware attacks so that you can protect your institution, finances and reputation.

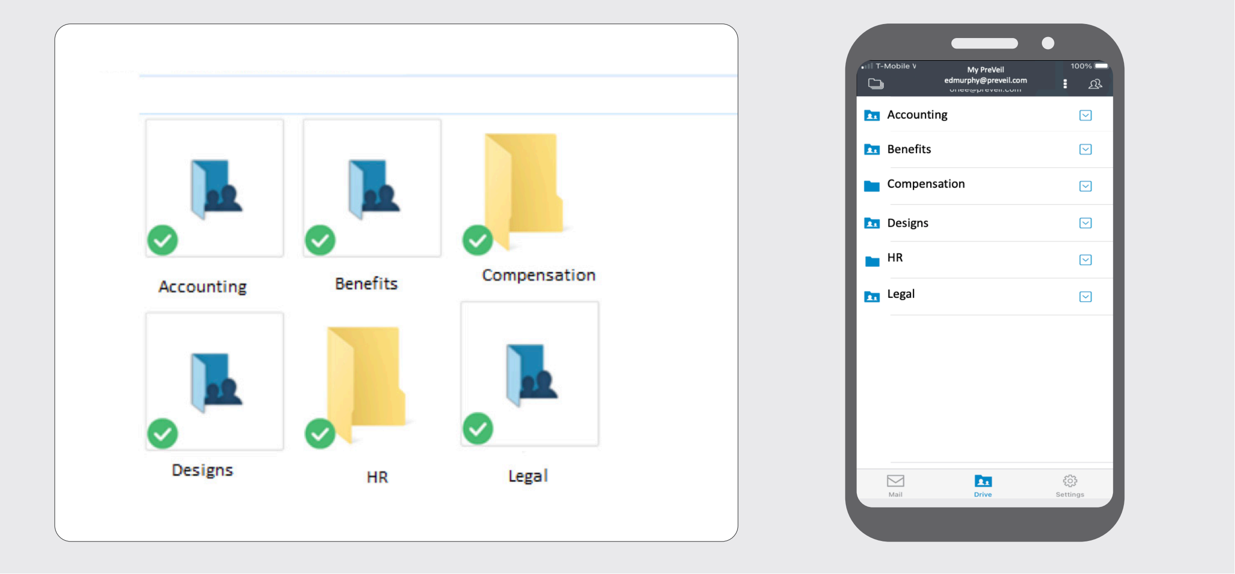
PreVeil: Simple, Encrypted Cloud File Storage and Sharing

Institutions can quickly deploy PreVeil with no impact on their existing servers or IT infrastructure. There's no need to rip and replace existing hardware or software, saving significant time and costs compared to typical installations.

From there, you secure your files and data by simply dragging and dropping them into **PreVeil Drive**, where they are automatically encrypted and stored in the cloud. With this simple action, your institution gains world class security and ransomware protection. Note that system files not moved into PreVeil folders remain unprotected.

Users can access files from their computers or mobile devices and share and unshare them both inside and outside their organization, as shown in Figure 1 below. PreVeil Drive works with Windows Explorer, Mac Finder, and on browsers.

Figure 1: PreVeil Drive: Sharing and storing files



How PreVeil protects your institution

PreVeil is far more than a cloud backup solution. It's built on Zero Trust principles, which assume that cyberattacks are inevitable: rather than focusing on preventing attacks, a Zero Trust mindset assumes that breaches will occur and focuses on protecting your data resources instead.[3] PreVeil accomplishes this through a design that addresses each of your institution's cyber vulnerabilities, as summarized here:

PreVeil Feature	How it Works
Neutralize ransomware attacks	PreVeil retains all prior versions of your files on an entirely separate system, letting you quickly restore your data to its most recent uncorrupted version in the event of a ransomware attack. Data is never lost and there's no need to pay off cybercriminals.
No passwords to steal	Attackers often hack passwords to access data and files and install ransomware. With PreVeil, there are no passwords to guess or steal. Instead, PreVeil uses secret unguessable cryptographic keys stored on your devices. Keys are automatically generated—no need for you to create or remember them.
Server breaches yield only gibberish	Unlike other file sharing services, data on PreVeil servers always stays encrypted and can be decrypted only on users' devices. Even if attackers breach PreVeil servers they will get only gibberish. No one but the intended recipient can ever read users' files and emails—not even PreVeil. This technique is called end-to-end encryption, widely considered the gold standard of cybersecurity.
Secure even if administrators are compromised	Hijacked or rogue administrators represent a significant risk because they typically have the ability to access your entire institution's files and emails. With PreVeil, data is secure even if an admin is compromised. That's accomplished by PreVeil's Approval Group feature, which is consistent with CISA's principle of least privilege to prevent ransomware attacks. Admins have to get approval from a pre-designated group of people within your business before accessing other users' information. Approval is a critical but seamless process that stops the spread of ransomware in your network.
PreVeil comes with encrypted email too	**PreVeil Email** automatically encrypts your emails so you can communicate securely with others inside and outside your organization. Even if your other servers are attacked and compromised, PreVeil Email allows you to continue to communicate internally because it's a separate system on a separate network. PreVeil Email works seamlessly with the systems you already use, namely, Outlook, Gmail, and Apple Mail. Users keep their regular email address, which keeps it simple.
Encrypted Logs	All user actions are logged in case it's necessary to troubleshoot an issue. The logs allow visibility throughout your network and its devices, enabling constant monitoring and assessment of your security status. The logs are encrypted on PreVeil servers so that only authorized administrators can review them.
Unlimited storage on Amazon Cloud	All data is end-to-end encrypted and stored on the Amazon Cloud. A fixed monthly price gives you all the storage you need.

[3] For a clear and understandable explanation of the Zero Trust mindset, see PreVeil's brief, *Zero Trust: A better way to enhance cybersecurity and achieve compliance*.

PreVeil's solutions, in combination with modern IT security practices, will defend your institution from attacks by sophisticated ransomware criminals. PreVeil understands that many colleges and universities may need to work with consultants to implement modern security practices. To that end, PreVeil has built a partner community of more than 100 organizations with cybersecurity expertise. Coordinated access to this specialized partner community will streamline your efforts to guard against ransomware, giving you the peace of mind you need to focus on keeping your institution running smoothly.

Operational continuity in the event of a ransomware attack

PreVeil helps your institution recover quickly in the event of a ransomware attack. You'll need to take these actions:

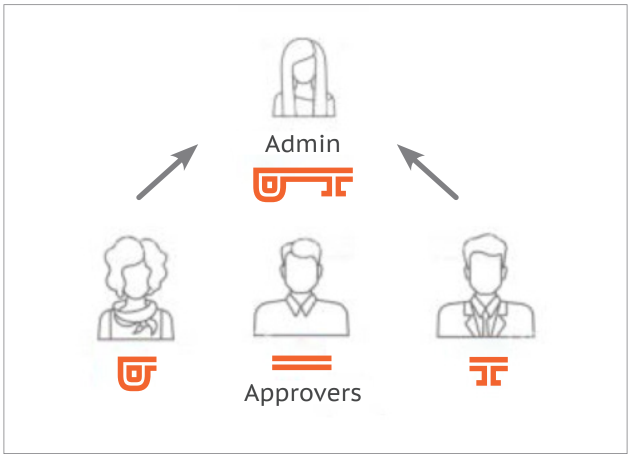
FIRST, find the source of your network breach, get the attackers out of your network, and remediate the deficiencies that enabled the attack. You'll also most likely need to reinstall basic systems on your affected computers. These steps can be difficult and may require the help of cybersecurity forensics experts, a topic beyond the scope of this paper.

NEXT, contact PreVeil support to roll back to the most recent versions of all your files and data. The good news is that PreVeil securely stores all versions of all your files and data on an entirely separate system, and so your most recent uncorrupted versions are readily accessible.

FINALLY, you can recover all of your users' keys (PreVeil's alternative to passwords) via PreVeil's Approval Group feature. As described above, administrators' access privileges are safeguarded by setting up a group of people within your organization, a pre-set number of whom need to approve administrators' access to other users' data. Each member of the Approval Group is given a shard of an automatically-generated cryptographic key that, when combined, give administrators the access they have requested, as shown in Figure 2.

It is critical that Approval Group keys be safeguarded, ideally by simply copying them to the PreVeil app on your mobile phone. PreVeil stores Approval Group keys in a secure admin-protected directory on your Mac or Windows computers. If those computers are attacked by ransomware, your phone can be used to readily recover the Approval Group keys. The Approval Group can then assist with recovering all of your other users' keys.

Figure 2: PreVeil Approval Groups: Admin access only with complete key



Finally, PreVeil comes with an encrypted email system that you can use to securely communicate with others inside and outside your organization. Unlike your main email system, you can trust PreVeil Email because it's a separate system that runs on a separate network—which, importantly, enables you to continue to communicate internally in the event of a ransomware attack. This ability is crucial to your institution's quick recovery.

Conclusion

We live in a world where cybersecurity breaches are inevitable. The realistic course of action for your institution is to assume there will be a breach and focus on neutralizing its impact. PreVeil is unique in that its world class security does just that: it protects your institution even when attackers successfully break into your systems. And while PreVeil defends your networks with state-of-the-art security, it's also simple to deploy, easy to use, and affordable. In fact, PreVeil is free for individuals. For institutions that need to secure their data and files, PreVeil is remarkably affordable.

To learn more about how PreVeil can help you secure your college or university with military grade security at an affordable price, contact us at **preveil.com/contact** or +1 (857) 353-6480.

PC PCMAG.COM EDITORS' CHOICE

Best System for Encrypted File Sharing and Email

Best System for Privacy

About PreVeil

PreVeil makes encryption usable for everyday work. PreVeil Drive works like Dropbox for file sharing, but with far better security. PreVeil's encrypted email works with existing apps like Outlook or Gmail, letting users keep their regular email addresses. All documents and messages are encrypted end-to-end, which means that no one other than intended recipients can read or scan them—not even PreVeil. PreVeil also retains every version of all your files and correspondence so that the most recent uncorrupted versions can be readily recovered in the event of a ransomware attack. PreVeil is designed for any size institution, from small colleges to large research universities. Visit www.preveil.com to learn more.

PREVEIL

September 2021