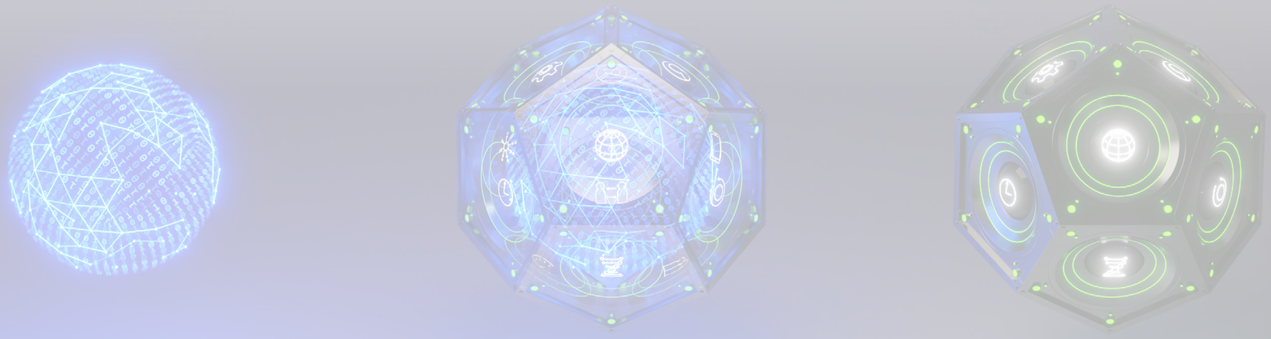
keyavi



How to Stop Ransomware In Its Tracks Now

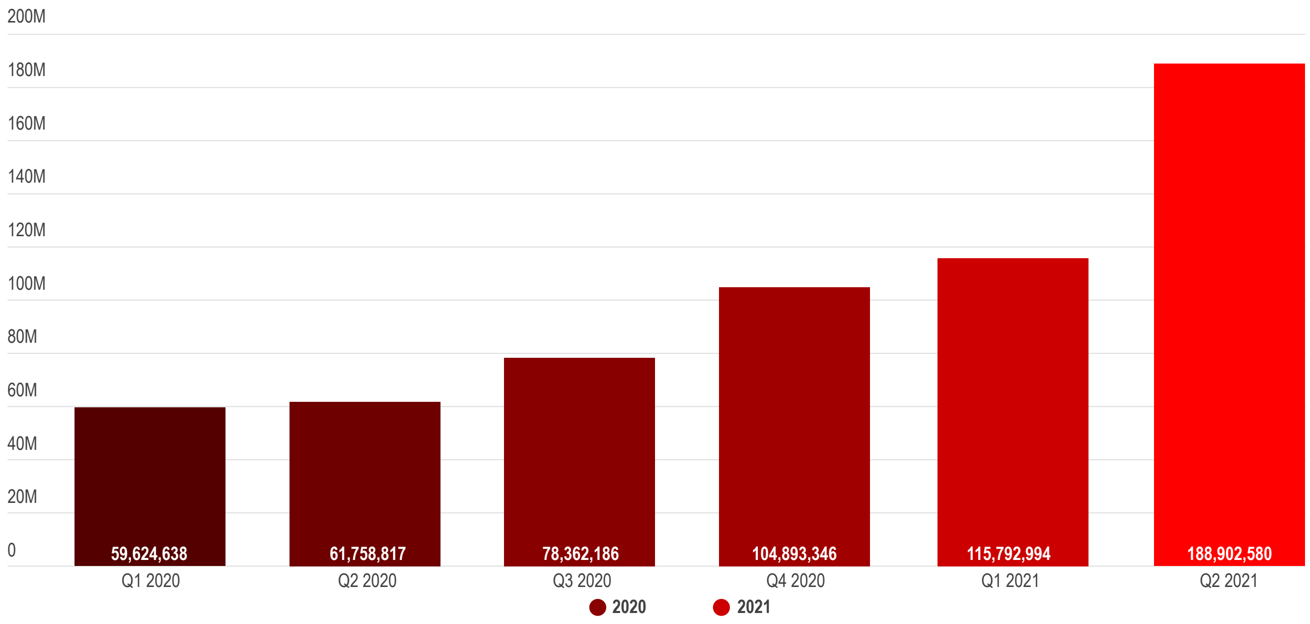
Groundbreaking Self-Protecting Data Technology Deals a Death Blow to Cyber Crime's Assault on Your Crown Jewels

Contents

Introduction

Ransomware attacks have reached crisis levels, and organizations everywhere are under siege.

Ransomware Growth By Quarter



Source: SonicWall 2021 Mid-Year Update Cyber Threat Report

Large payouts, coupled with a relatively low risk of being caught, are encouraging criminals to launch these attacks with greater impunity.

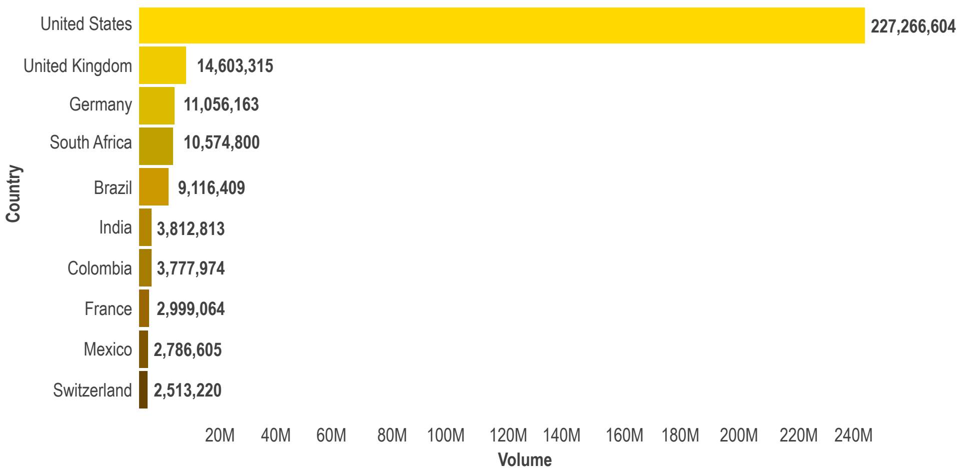
The bad actors behind these attacks are highly organized and well-funded. They leverage phishing and social engineering schemes, custom hacking software and other technical weaponry on a growing number of people and digital targets to hijack confidential data on a massive scale. The FBI[1] compares ransomware attackers to terrorists who pose increasingly greater data loss, financial and other risks for businesses, government agencies and critical national infrastructure.

While high-profile attacks against Colonial Pipeline, JBS Foods and Kaseya, Ltd. provided months of fodder for news outlets, the reality is that ransomware attacks are woefully under-reported and their ramifications significantly underestimated.

In 2020, the FBI received 2,474 ransomware complaints, though the agency admits this is likely a mere fraction of the true scope of attacks because the data captures only those individually reported to its Internet Crime Complaint Center (IC3).[2,3] According to a 2021 SonicWall report, ransomware attacks skyrocketed 62% worldwide and 158% in the U.S. alone.[4] As double extortion attempts escalated between the first and second quarters of 2021, ransomware attacks surged 288%, according to NCC Group researchers.[5]

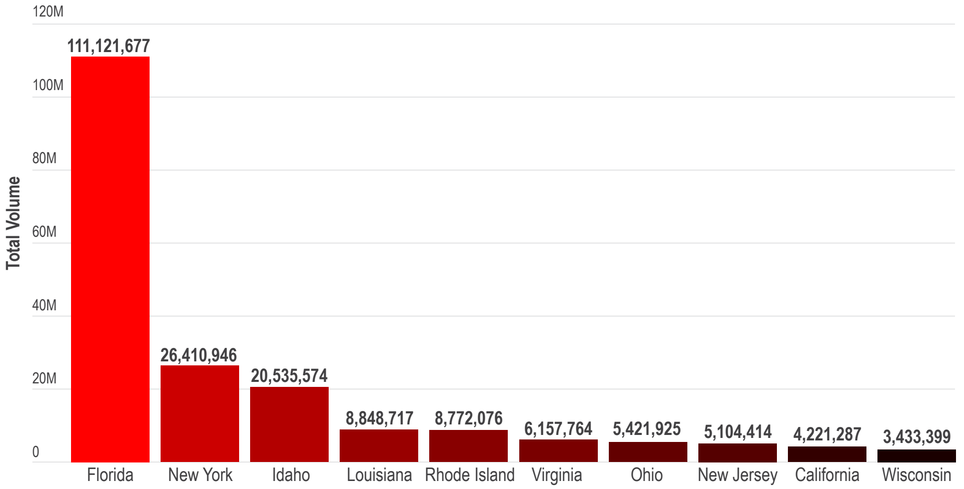
Unfortunately, the pace and volume of attacks are intensifying.

2021 Ransomware Volume | Top 10 Countries



Source: SonicWall 2021 Mid-Year Update Cyber Threat Report

2021 Ransomware Volume | Top 10 U.S. States



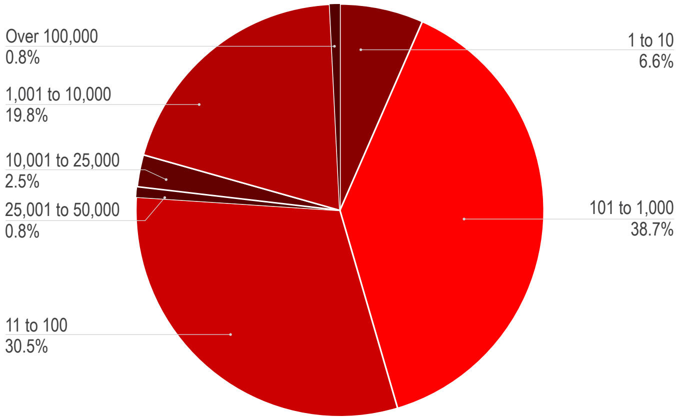
Source: SonicWall 2021 Mid-Year Update Cyber Threat Report

So why has ransomware become such a plague? Because it's all about the money — for all the wrong people. Ransomware has become a major source of very easy money for cyber criminals who know where & how to exploit vulnerable networks and exfiltrate unprotected data.

No one is immune. The Cybersecurity and Infrastructure Security Agency (CISA) continues sounding the alarm with alerts about ransomware criminals targeting pipelines and critical national infrastructure, healthcare, city and state governments, technology companies, schools and many other sectors – especially around holidays and on weekends.[6] As these threats grow in magnitude, indiscriminately targeting businesses of virtually every size across a wide range of industry segments, every organization should pay attention.

Small and mid-size businesses are among the hardest hit.

Distribution by Company Size (Employee Count)



Rather than maintain their own IT teams, these companies often hire outside managed service providers (MSPs) to handle their technology needs. During the July Fourth holiday weekend this year, for example, a ransomware supply chain attack on Kaseya, an IT solutions provider for MSPs, rippled through to an estimated 1,500 small and medium-sized businesses. Although the full scope of downstream victims isn't fully known yet, some experts believe the numbers of small and mid-size businesses impacted could be much higher.[7]

"More than 75% of ransomware attacks occur at companies with fewer than 1000 employees."

Source: Coveware 7/23/21 Blog

For many small businesses that may already be struggling financially, ransomware could prove catastrophic. Criminals hit the pocketbooks of these organizations – from libraries and school districts to police and fire departments – that are unable to either pay ransom demands or recover their data after a devastating attack.

Even more alarming is that cyber threat actors understand the growing reliance of organizations on MSPs and take full advantage of opportunities to attack them.[8,9]

Larger companies with deeper pockets and potentially greater amounts of data to hijack attract the most attention from ransomware criminals and the biggest news headlines. Yet ransomware attacks are getting more expensive for enterprises as emboldened criminals demand mega-million sums in return for hijacked data. The average ransom paid by organizations increased from $115,123 in 2019 to $312,493 in 2020 – a 171% year-over-year increase, according to the latest Unit 42 Ransomware Threat Report.[10] Between 2015 and 2019, the highest ransomware demand was $15 million. By 2020, that demand had already reached $30 million.[11]

"The average ransom paid by organizations increased from $115,123 in 2019 to $312,493 in 2020 – a 171% year-over-year increase."

Attacks Have Downstream Ramifications

These attacks often have ramifications far beyond dollars, reputational damage or rising cyber insurance premiums.

When a ransomware attack hit a major U.S.-based telemarketing firm, for example, the company was forced to lay off 300 employees just days before Christmas. The Colonial Pipeline attack led to gasoline panic-buying and shortages along the entire eastern seaboard of the U.S. for weeks.

Ransomware is also placing people's health and their lives at risk. An attack on the University of Vermont Medical Center last November delayed chemotherapy treatments to cancer patients. In another ransomware attack on a hospital in Dusseldorf, Germany, emergency-room staff were forced to divert an ambulance to a different hospital because its IT systems had been hijacked. The attack delayed the patient's treatment by an hour, leading to her death shortly thereafter.[12]

The Ransomware Playbook is Expanding

Ransomware gangs are becoming more ruthless and evolving faster than the cybersecurity industry can respond. Criminals have moved beyond crypto mining and encrypting a victim's data to exfiltrating and reselling that same stolen data to the highest online bidder. They are also extorting the victim's customers, third-party suppliers and employees with threats to publicly disclose the same stolen data.

During the first four months of 2021, six ransomware variants – Ryuk/Conti, Sodinokibi/REvil, DoppelPaymer, Clop, Darkside and Avaddon – are believed to be responsible for nearly 300 attacks costing organizations across the manufacturing, transportation, construction, education and healthcare industries more than $45 million.[13] Other notable variants include Lockbit, RagnarLocker and RansomExx.[14]

The rise of ransomware-as-a-service (RaaS) groups also enable different threat actors with varying skills to apply variants in their attacks. Others either own, operate or distribute malware for conducting these attacks.[15]

The cybercrime underground operates a dark web marketplace of its own, where ransomware operators turn to partners and affiliates seeking more access points into vulnerable systems for phishing and ransomware exploits. Initial Access Brokers help find those vulnerabilities and, like middle managers, list those access points along with other stolen credentials for sale on the dark web. For example, a data-theft extortion marketplace called Marketo Data Leak Site – not to be confused with legitimate marketing software Marketo – focuses on selling compromised data to the highest bidder.[16]

As the highly lucrative ransomware economy expands, more gangs are regrouping and rebranding themselves to evade detection and law enforcement. At the same time, they're joining forces with other gangs so that their proverbial golden goose is even more profitable. They leverage a myriad of methods to gain footholds in victim environments and continue to find innovative means of access. Meanwhile, internal IT teams remain stuck in a reactionary cycle of Whac-a-mole in attempts to fix vulnerable internet-accessible endpoints as the attack surface increases along with malware outbreaks and ransomware threats.

If organizations continue giving into extortionists' demands to unlock their hijacked data, they are not only spreading the ransomware contagion but are also unwittingly funding criminals' development of next-generation malware.

From the CISO's Desk

T.J. Minichillo,
CISO & VP of Threat Intelligence

When COVID-19 engulfed the world last year, many organizations were forced to streamline operations, lower costs and rethink their IT strategies so that workflows among remote employees, customers and supply chains remained intact. At the same time, this highly distributed yet digitally interconnected environment introduced new, porous attack surfaces that sophisticated gangs of criminals were only too happy to exploit. When tools that were designed to keep data secure failed with catastrophic consequences for hundreds of enterprises and government agencies, the blame fell on technologists for relying on obsolete perimeter-protection strategies rather than viewing data-centric security as an essential driver of an organization's ecosystem.

As anyone victimized by a data breach or ransomware attack will attest, current approaches and tools for managing cybersecurity are broken. More boards of directors and CEOs are sleepless, worrying whether they've calibrated the right type and scale of security investment to safeguard data against a rising tide of criminal masterminds. They lean more heavily on their CISOs to build and maintain what they hope are hack-proof capabilities, only to discover – often too late – that confidential business, customer, employee or supply-chain information has been exfiltrated and being sold to the highest bidder on the dark web, negotiated for ransom or exposed publicly to cause brand or reputational damage.

Data breaches, phishing scams and ransomware attacks touch every aspect of modern life. The fallout from a data breach equates not only to lost company sales and revenue but damage to its reputation and even loss of critical intellectual property, such as confidential software code and product designs.

Security should never be viewed as a business "blocker" but as an enabler, supporting business processes and workflows in ways that boost productivity, growth and revenue.

Problem 1:
Traditional Cybersecurity Tools Don't Work

From application security to endpoint detection, cybersecurity has suddenly become a top priority for thousands of global CIOs.

The massive increase in cyber threats resulting from the shift to remote work during the COVID-19 pandemic as well as rising ransomware attacks have led to double-digit increases in integrated risk management technology spending.

Large enterprises plan to spend more this year on every category of information security and risk management, according to the latest Gartner forecast.[17] Worldwide spending on these technologies and services are projected to grow 12.4% to $150.4 billion this year. Spending is also expected to increase significantly for infrastructure protection ($24 billion), network security equipment ($17 billion) and identity access management ($14 billion).

On average, enterprises spend between $30 million and $50 million per year on cybersecurity tools that are powerless to combat ransomware. Unfortunately, no amount of money on obsolete cyber tools will deter ransomware attackers from exfiltrating data. Many traditional cybersecurity software and hardware products on the market today are technologically limited and overly focused on data loss protection, breach detection and data containment. That's one reason why global damage from cybercrime is projected to grow 15% year-over-year to $10.5 trillion by 2025.[18]

As the global attack surface grows every day, and with everyone's security perimeter now everywhere and anywhere data travels, being resilient to ransomware attacks takes on far greater importance. If the pandemic taught us anything, it's that staying nimble, flexible and elastic by adapting business operations on the fly is possible only if data-centric security is built into IT architecture from the start. Accurately detecting and mitigating security incidents as they arise so that business processes aren't interrupted while data remains safe from those incidents is the hallmark of a cyber resilient business.

Problem 2:
Your Data Can't Protect Itself

Data is the one constant in today's complex, continually evolving technology ecosystem. It's the currency of IT. And the secure, uninterrupted flow and sharing of data are the heart and soul of every organization's business. That's why protecting data must be every cybersecurity leader's top priority. Yet many have missed this wake-up call.

TechJury,[19] which gathers big data statistics, reports that every person in 2020 generated 1.7 megabytes of data per second, while internet users generate about 2.5 quintillion bytes of data every day. Much of that data remains vulnerable to breaches.

COVID-19 exposed not just the technological vulnerabilities of organizations everywhere, but the incredible dependencies we all place on free-flowing data to do our jobs and run our companies efficiently. In today's highly connected world, it's no longer a question of whether you or your company will be attacked by cyber criminals. It's a matter of when and how long it will take to detect, negate and recover from the intruders.

Defenseless, unprotected data in the hands of ransomware gangs is the oxygen that powers criminal business models. Recently, these groups have invented new ways of extracting revenue from stolen data long after the initial ransom demand or payout.

Ransomware today has evolved into a complex criminal enterprise involving a shifting, interlocking network of gangs and cartels, such as LockBit and Ragnar Locker, that work both jointly and independently to make money through extortion as well as by selling stolen data to third parties.[20]

Some, such as REvil, have even devised ways to earn passive income, selling the tools of their trade to other criminals in RaaS franchises.

Today, there are at least 100 ransomware variants for exfiltrating data being investigated by the FBI.[21] By 2031, ransomware is projected to cost companies $265 billion, with an attack occurring every 2 seconds, according to research firm Cybersecurity Ventures.[22]

Fortunately, there's a better solution.

3 Phases of Ransomware

Most people think ransomware attackers just lock and encrypt data as a one-time-only event. But ransomware has become far more pervasive, with attacks staged in three distinct phases.

Phase 1:
Entry, reconnaissance, and launch

The first phase of a ransomware attack is all about a criminal getting into an organization's system without the victim knowing it, then controlling that system without being detected for as long as possible.

In addition to leveraging publicly known vulnerabilities and remote desktop protocol services, a criminal typically obtains access to an IT network by introducing malware via a phishing email containing a malicious link or attachment that an employee is enticed to click on or open.[23] The attacker then gains initial access through the use of remote access trojans and other malicious tools to spy on its victim, scope out the system, disable security software and – most importantly – find and steal the organization's most valuable data. Defense evasion techniques enable a criminal to snoop and steal data undetected for weeks or even months.

At the end of Phase 1, an attacker will launch file-encrypting ransomware. In a vast majority of cases, this is the first time a victim even notices a security incident has occurred.

Phase 1 attacks are loss leaders for criminals because they must spend a considerable amount of their own money, time and risk before exposing their presence to a victim. Many ransomware criminals move on to the second and third phases of an attack because the prospect of a large payoff beckons.

Phase 2:
Making the victim pay

During this phase, attackers threaten to expose or auction a victim's stolen data if their ransom demands aren't met.[24]

Paying a ransom, however, doesn't end the problem. A recent study by Cybereason found that, although 46% of companies pay a ransom to regain access to their data, some or all of it is corrupted.[25]

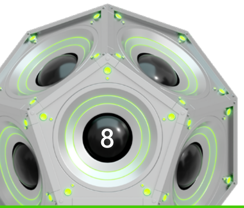
There's another aspect of a Phase 2 attack that makes it even worse for the unwitting victim. Criminals can keep copies of the same stolen data that a victim just paid a ransom to retrieve, store those copies elsewhere and then exfiltrate the data. They then continue to ransom copies of the stolen data back to the victim multiple times for even more money.

Phase 3:
Double extortion

For criminals, the third ransomware phase is their biggest money-maker of all.

Here, an attacker demands an even bigger ransom than during Phase 2 to prevent the sale or disclosure of a victim's data to third parties, customers or business partners. To up the ante, criminals will often require a victim to pay the ransom within hours or minutes as a timer ticks away.

Imagine a ransomware criminal threatening to expose or sell every shred of your organization's exfiltrated data on the dark web — from confidential personnel files and customer lists to patents or other intellectual property — if you, the victim, refuse to pay up. Suddenly, all those data backups and data recovery plans become worthless as the nightmarish realities of reputational damage, compliance fines and potential lawsuits hit home.



The Solution: Self-Protecting Data

All modern security systems share one fundamental flaw: they can't guarantee sensitive data won't fall into the wrong hands. This simply isn't possible with current security protocols, which fall into two main categories:

Category 1
Attempts to keep data contained

Identity and access management systems, mobile device management, sensitive data encryption, cloud access management and storage are all important cybersecurity tools, but they're not perfect. An attacker only needs to get through one of them to penetrate a network and steal data.

Category 2
Attempts to control a growing, continually evolving threat landscape

Cyber criminals continue to take full advantage of a greatly expanded attack surface as well as pandemic-related fears by luring unsuspecting remote- and office-based workers into clicking on malicious email links, seeking to spread malware and exfiltrate individual and company data. Threat intelligence, incident response and forensics tools and technologies – coupled with event management and response solutions (SIEM and SOAR) – are necessary for monitoring today's cyber threat landscape. But as a company's security tech stack grows, so do the endpoint gaps that criminals could also penetrate.

From the CEO's Desk

Elliot Lewis,
Co-founder & CEO

Data security shouldn't be about putting up higher walls and deeper moats to stave off hordes of attackers. Those walls, no matter how high or how thick, won't defend against adversaries who manage with greater frequency and sophistication to penetrate networks and steal data without anyone detecting the intrusion, sometimes for years.

Nor should data security be about piling on more tools onto your tech stack in the hopes of making your business more secure. Solving the problem of leaky data right from the get-go requires completely re-thinking your strategy for securing data. True cyber resilience is about helping a business grow by providing visibility into how data is used, how it interacts with your customers, your ecosystem and operations. Instead of data being a business risk, it should be a contributor to business growth.

Data is the lifeblood of every business. It flows through an organization's circulatory system every second of every day, with a myriad of internal and external touches needed for critical business and work-related functions. It fuels actionable knowledge to achieve business goals. And it powers pathways to innovation.

These twin rivers of data have become the currency of choice for cyber criminals. Every touch point in an organization's data flow, or throughout an individual's connectivity to the Internet, represents potential points of data capture by bad actors.

Unlike other security systems, self-protecting data strikes at the heart of ransomware's business model: its money-making machinery. The advent of self-protecting data eliminates these sources of income – and with it, the incentives that draw most of the bad actors into this business. When attacks require the same amount of work but become far less profitable, the motivation to launch them will fade, forcing attackers to turn their attention to other exploits.

News about the latest attacks shows how quickly trust has eroded in a majority of network monitoring and security technologies on the market today, simply because those obsolete tools failed to secure data. Yet, the knee-jerk reaction of many companies is to pay off the bad actors and keep piling on even more obsolete tools out of fear that criminals will continue penetrating their system. The one assumed premise – that data can't protect itself – never enters into the equation.

> **"The one assumed premise – that data can't protect itself – never enters into the equation. But it should."**

But it should.

A truly cyber resilient organization prepares for the inevitable ransomware attack using a combination of data-centric security tools, policies and people that quickly detect and mitigate cyber attacks without interrupting the ebb and flow of business operations.

More than a decade ago, Keyavi's co-founder and CEO, Elliot Lewis, foresaw the devastating effect that unprotected "data in the wild" resulting from an accidental leak or breach would have on people and organizations everywhere. So, he set out to simplify an amorphous IT ecosystem into one self-protecting, self-intelligent object – data itself.

Under development for nearly 10 years, Keyavi's patented application programming interface (API) platform is so revolutionary that it's stopping cyber criminals in their tracks. They can't open data if it's infused with Keyavi's self-protecting, intelligent, self-aware technology. This breakthrough solution wraps data with multiple encryption layers so that no single layer can be compromised without triggering protection mechanisms in the surrounding layers.

Keyavi's previously unimaginable data security innovation is unlike anything else on the market. For the first time, data is now able to automatically think for itself and protect itself – no matter where it goes in the world, no matter who has it, where it's stored or how many copies exist.

Instead of trying to keep data contained, data is now its own fortress. As a result, data can safely travel or reside anywhere in the world because everywhere Keyavi's self-protecting, intelligent and self-aware data goes, it follows the rules of the individual or organization that owns it.

How Self-Protecting, Intelligent, Self-Aware Data Security Technology Works

Multi-layered encryption and embedded policies define who can access the data as well as when, where and how.

Keyavi enables data owners to activate multiple policies, geo-fencing and time embargo capabilities on every piece of their data to prevent unauthorized users from opening their data on unauthorized devices, thus mitigating the risk of threat actors using stolen data in any extortion attempts. Now, wherever and whenever an intelligent data file or folder is stored or sent anywhere in the world, it knows to open only for the person who's authorized to access it. At the same time, this intelligent data automatically reports back to its owner in near-real time where it is, who has it and what device it's on.

Online & Offline Access: Keyavi's award-winning technology is platform, transport and application agnostic. It works online, and it works offline – everywhere and anywhere data travels.

Easy to Use: Seamless for all users.

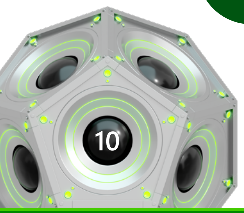
Platform- & Transport-Agnostic: Embeds into the data itself, completely independent of any delivery method.

On-the-Fly Policy Editing: Implements owner's policy changes, including authorized users and devices, time periods and geo-location every time the data is accessed.

Intelligent Directory: Automates quick, organization-wide protection of critical data while enforcing internal security policies on that data.

Advanced Embedded Data Protection Built on Industry Standards: Patented, multi-key encryption technology based on industry standards such as PKI, AES and CryptoAPI protect data anywhere it goes for any length of time.

Deep Forensic Logging, Possession and Custody Controls: Record the complete lifecycle of Keyavi-infused data for the owner – from creation and usage to storage and destruction. This "chain of custody" and compliance reporting captures and records every access attempt with unique user, device and geo-location information. It also reports all data activity live to the owner, anywhere data goes.



Keyavi-infused data can also sense the presence of endpoint protection solutions in order to stay off infected devices. Keyavi's technology uses a proprietary multi-level "wrapper" system with patented multi-key, multi-layered encryption that:

Protects and encrypts
data content, whether individual files or groups of files.

Creates and applies
policy and rule sets embedded into a data "wrapper" with more encryption – encompassing both the data and its encryption keys

Encrypts the policy sets,
making data accessible only under specific rules set by the data owner, including geo-location, the identity of an authorized recipient, specified devices or services or platforms, time/day access embargoes, digital rights management and any additional policies the owner applies.

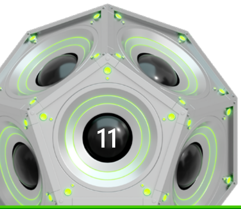
Intelligent data can only be accessed when all of the owner's permission parameters are satisfied, which can be tailored to each owner's policy settings. A data owner can allow or prevent access by geo-location, such as company site and home office or at a street, state or country level. An owner can also choose to change access permissions or revoke access completely from any or all recipients at any time – for the life of the data, wherever it is stored – by simply changing permissions from their device.

Keyavi-infused data will also follow an owner's commands in perpetuity. By merely hitting one button on any device, a data owner can change policies on the fly for any piece of data ever sent to anyone or anywhere. The owner can also reassign data access rights to someone else or delete every piece of intelligent data he or she owns – no matter who has it, where it's stored, or how many copies were made. If data travels outside its policy-approved location, it will refuse any further interaction. It can also self-delete or simply stay encrypted, all while reporting its whereabouts back to the data owner.

If intelligent data assesses and approves its location, it will then proceed to confirm whether the recipient's rights have been revoked or changed. If a recipient is still allowed access, the data will unlock its policy models and systematically process its rulesets to determine its next course of action. Only after all other checkpoints have been OK'd will data then use another content key to allow access.

Keyavi's technology plugs-and-plays easily with any IT hardware, any software or any device by augmenting any technology solution set for any market or industry vertical. Because it is centered around a rich, self-describing REST API, the company's solutions can be customized by developers for infusing Keyavi data protection into their OEM and enterprise applications.

A desktop app allows Keyavi to access over 50 pieces of forensics data in the underlying operating system that can be leveraged for policy-based security. For example, the desktop app will enable a policy that allows a file containing company secrets to be opened only by a specific user on a specific device.



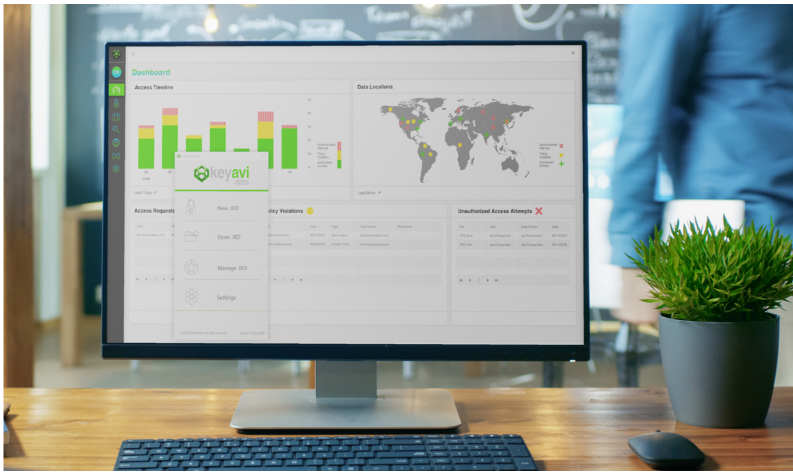
Users of this innovative technology – either as an API, a desktop client software product, mobile app or web client – can now secure data without having to rely on a specific platform, device, application or operating system.

On a Desktop

Every fully licensed user receives a desktop client, robust Microsoft Office plug-in and access to four mobile apps, a free online viewer and a web client. The technology plugs-and-plays seamlessly with O365 applications such Excel, Word, PowerPoint and Outlook. Users can fully secure their files at the mere click of a button.

Keyavi's Intelligent Directory service is deployable across an organization to immediately protect critical data. Installing Intelligent Directory on an existing cloud or device storage system (such as OneDrive, Dropbox, Box) automatically applies and enforces a security team's policies onto all the data in those locations.

The desktop app also enables Keyavi to access more than 50 elements in the underlying operating system that can be leveraged for policy-based security. For example, the desktop app will enable a policy that allows a file containing confidential data to be opened only by a specific user, on a specific device, at a pre-determined time and place.



Keyavi never accesses, stores or otherwise intercepts anyone's data. Our lightweight Keyavi API, mobile apps and viewer enable the highest level of data protection, run seamlessly in the background and require minimal memory.

Freedom to Customize

With its mobile apps and web client, the company also enabled agent and agent-less capabilities on any mobile device.

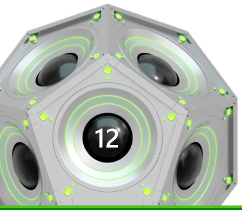
With Keyavi's API for enterprise customers and OEM partners, developers can customize comprehensive data protection into their own applications, products, firmware and services. The lightweight API allows developers to integrate data protection into existing applications and data workflow within the client, server, gateway or cloud.

No Internet? No Problem!

Keyavi's strong encryption and access control policies ensure that data is self-protected and secure, even when data goes offline.
When accessing Keyavi-infused data without internet connectivity, a "default safe and closed" policy can be applied, including conditional time-window or geo-location allowances to enable offline access for a limited period of time.

Privacy and Protection at the Data Layer Itself

With multiple security policies, encryption layers and classifications infused directly into data itself, no single layer can be compromised without triggering the data's self-protecting and privacy mechanisms. For example, when a user shares data that requires a myriad of federal or other regulatory compliance controls, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Payment Card Industry Data Security Standard (PCI DSS), Keyavi's technology allows a user to apply those controls easily and quickly.



On a Mobile Device or in a Web Browser

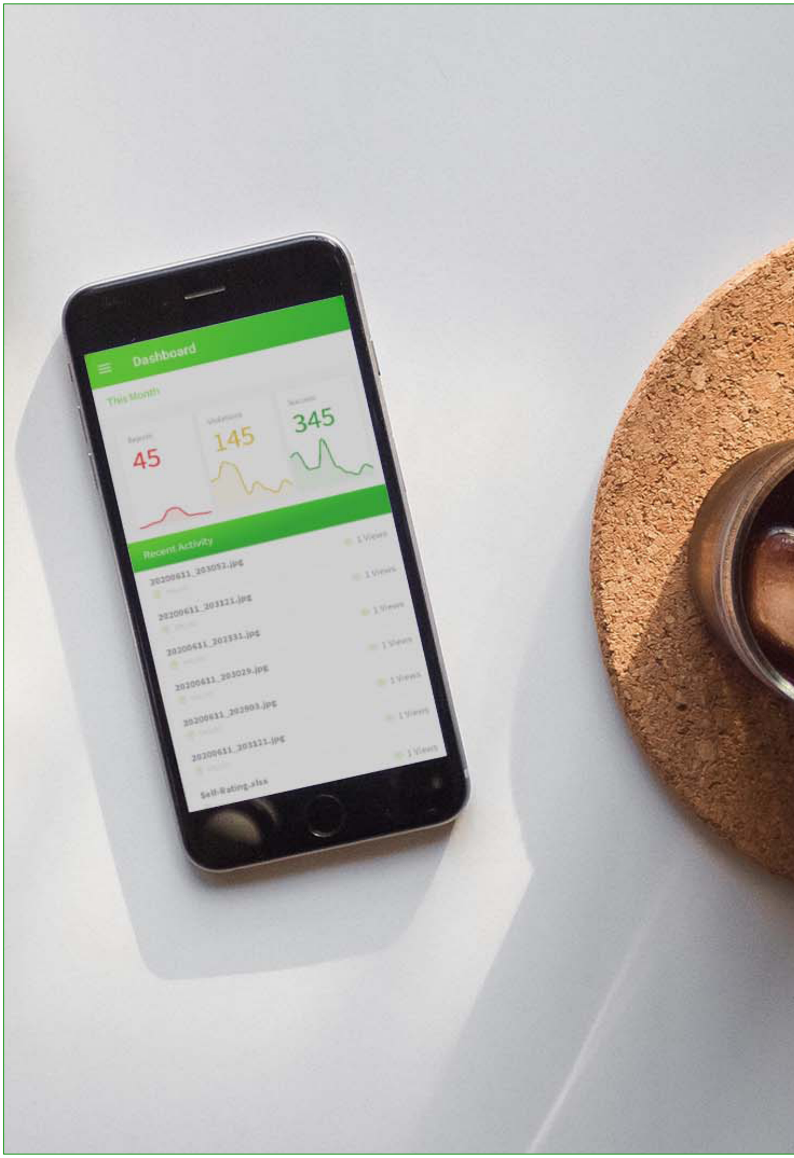
Keyavi's four mobile apps, online viewer and web client provide on-the-go-access with the same power and functionality as a full desktop product suite. The web client looks and behaves like the company's desktop software product, with the same security protocols but with additional browser-specific functionality.

To open any Keyavi-protected files on a mobile app or online, a user need only download and install any of the iOS, Android or Microsoft apps or open a web browser once. Android, Apple and Microsoft automatically point mobile users to the right app for downloading, then open the intelligent Keyavi file using the company's free viewer.

The online viewer, which operates seamlessly in the apps' background, allows an authorized recipient of the intelligent file to access it in read-only mode in its native application on a mobile device. Anyone who's authorized to open a Keyavi-secured file can now simply double-click on it – even if the recipient doesn't have a Keyavi user license or has never seen a Keyavi-infused file before. If, for example, a Microsoft Word file is protected at the outset with Keyavi's technology, the recipient of that file can easily view it in Word if their mobile device has the appropriate Windows plug-in and mobile app installed.

Once a Keyavi app is installed, a licensed user can transform any type of data file into intelligent data – whether it's an email, Word document, text file, spreadsheet, pdf, video, or any other file type – and infuse powerful controls into that data: who's allowed to see it, when and where it's accessed, by whom and on what devices. They can then send those multi-layered, encrypted files to anyone inside or outside their organization, knowing their data will stay under control even after leaving their possession.

Before sharing an intelligent Keyavi-infused file, users can also grant or refuse access for specific individuals or groups of people by geographic location as well as set specific date and time limits for accessing the file. Because the owner can also change or revoke permission parameters on the fly from his or her smart device or computer at any time, the data always stays under the owner's control, regardless of where the data is located or who has it. Should an unauthorized user try to gain access or steal data without appropriate permissions, the data automatically self-protects.



"A licensed user can transform any type of data file into intelligent data – whether it's an email, Word document, text file, spreadsheet, pdf, video, or any other file type."

Keyavi + Partner Ecosystem Solutions

Keyavi is expanding its patented data security capabilities with a new partner ecosystem that encompasses best-in-class anti-virus/anti-malware experts at detecting and stopping advanced Phase 1 ransomware attacks by continuously monitoring endpoint files and processes across an entire network.

Keyavi is also partnering with top-performing partners to help their customers bolster their defenses against a growing onslaught of ransomware attacks while simultaneously lowering their cyber risk.

Summary

Ransomware criminals are making big money off your data. Isn't it time you turned the tables on them with a hijack-proof solution?

Today, data can think for itself and protect itself automatically, no matter where it goes in the world, no matter who has it, no matter where it's stored, and no matter how many copies exist.

Keyavi's technology — the first of its kind anywhere — lets you infuse your data with self-protection tools and intelligence embedded with your data, at the data level. You have total control of your data, however and wherever you want, no matter where it goes, no matter where it's stored, no matter who has it.

Up until now, the entire cyber market based its security approach and tools on one premise: that data could not protect itself. It's the one premise that ransomware criminals count on – until now! Keyavi's platform stops ransomware attackers cold by infusing data with intelligence, self-protection and self-awareness. We don't treat the symptoms of data loss. We make data smart. Now the bad actors can't access, steal or ransom your data if it's infused with our award-winning, patented technology.

Isn't it time to re-think your cyber resilience playbook – one that gives you total control of your data's destiny, yet is both elegant and simple to execute?

We can help rewrite your ransomware playbook with a sure-fire offense right from the get-go.

Learn more about self-protecting, intelligent and self-aware data security technology. Sign up for a webinar or take a test drive during a demo at www.keyavi.com

Keyavi Data. For the ultimate in data security peace of mind.

About Keyavi

Headquartered in Durango, Colorado, Keyavi's self-protecting, intelligent and self-aware cybersecurity technology enables an individual piece of data to think for itself; secure itself; control where, when and who is allowed to access it; refuse access to unauthorized users; stay continually aware of its surroundings and automatically report back to its owner – with all these capabilities built into the data itself. The company's API platform and a full suite of applications riding on that platform also provide data owners with powerful controls to allow, revoke or deny access to their information – no matter who has it, on any platform or device, regardless of how many copies exist.

Under development for years before launching in 2020, this award-winning, multi-patented technology is so unique and innovative that leading industry analyst firm Omdia designated "self-protecting data solutions" as a new cybersecurity industry category, with Keyavi as the clear leader. Keyavi's easy-to-use yet robust solution delivers the ultimate in peace of mind for public and private organizations, their remote workforces and partner ecosystems in solving the security challenges of controlling confidential and intellectual property from data leaks, breaches and ransomware.

To learn more about Keyavi and its breakthrough technology, visit keyavi.com/our-technology.

Follow Keyavi on LinkedIn, Vimeo and Twitter.

keyavi.com

DISCLAIMER

This publication is provided "AS IS" and all express or implied conditions, representations and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaimers are held to be legally invalid. Keyavi Data Corp. shall not be liable for incidental or consequential damages in connection with furnishing, performance, or use of this publication. The information contained herein is subject to change without notice.

[1] FBI: America Under Cyber Siege 7/7/21 https://www.fbi.gov/news/testimony/america-under-cyber-siege-preventing-and-responding-to-ransomware-attacks

[2] 2020 Internet Crime Report, FBI Internet Crime Complaint Center (IC3) https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[3] Testimony of Bryan Vorndran, Asst. Dir. FBI Cyber Division, Senate Judiciary Committee https://www.judiciary.senate.gov/imo/media/doc/Vorndran%20-%20Statement.pdf

[4] 2021 SonicWall Cyber Threat Report https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyber-threat-report.pdf

[5] NCC Group Research Intelligence and Fusion Team (RIFT) Analysis https://newsroom.nccgroup.com/pressreleases/ncc-group-reveals-threefold-increase-in-targeted-ransomware-attacks-in-2021-3124798

[6] CISA Official Alerts & Statements https://www.cisa.gov/stopransomware/official-alerts-statements-cisa

[7] Senate Testimony: America Under Cyber Siege https://www.judiciary.senate.gov/meetings/america-under-cyber-siege-preventing-and-responding-to-ransomware-attacks

[8] MSPs Report Ransomware is Still the #1 Malware Threat Affecting Businesses; Cost of Downtime Nearly Doubles Since 2019 https://www.businesswire.com/news/home/20201117005156/en/MSPs-Report-Ransomware-is-Still-the-1-Malware-Threat-Affecting-Businesses-Cost-of-Downtime-Nearly-Doubles-Since-2019

[9] [1] 2020 Internet Crime Report, FBI Internet Crime Complaint Center (IC3)CISA Insights: Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf https://www.cisa.gov/publication/guidance-msps-and-small-and-mid-sized-businesses

[10] 2021 Unit 42 Ransomware Threat Report https://unit42.paloaltonetworks.com/ransomware-threat-report-highlights/

[11] Ibid.

[12] Police Investigating Hospital Cyber Attack Death https://fortune.com/2020/09/23/cyberattack-death-dusseldorf-germany-ransomeware-ambulance/

[13] eSentire Ransomware Report https://www.esentire.com/resources/library/six-ransomware-gangs-claim-290-new-victims-in-2021-potentially-reaping-45-million-for-the-hackers

[14] Ransomware Watch https://www.ransomwatch.org/

[15] Ibid.

[16] Marketo: A Simple Return to Extortion https://www.digitalshadows.com/blog-and-research/marketo-a-return-to-simple-extortion/

[17] Gartner Worldwide Security and Risk Management Forecast https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

[18] Cybersecurity Ventures Global Ransomware Damage Costs https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

[19] TechJury Blog https://techjury.net/blog/big-data-statistics/

[20] Cybereason Rise of Double-Extortion Shines Spotlight on Ransomware Prevention https://www.cybereason.com/blog/rise-of-double-extortion-shines-spotlight-on-ransomware-prevention

[21] FBI Investigating 100 Ransomware Variants https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/fbi-investigating-100-ransomware-variants/

[22] Cybersecurity Ventures Global Ransomware Damage Costs https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

[23] Ransomware: These are the two most common ways hackers get inside your network https://www.zdnet.com/article/ransomware-these-are-the-two-most-common-ways-hackers-get-inside-your-network/

[24] REvil Ransomware Gang Starts Auctioning Victim Data – Krebs on Security https://krebsonsecurity.com/2020/06/revil-ransomware-gang-starts-auctioning-victim-data/

[25] Most Businesses That Pay Off After Ransomware Hack Hit With Second Attack https://www.newsweek.com/most-businesses-that-pay-off-after-ransomware-hack-hit-second-attack-study-1601266