PRESIDIO® SentinelOne®

Don’t Get Held for Ransom

Design the right security infrastructure to detect, mitigate, and prevent ransomware attacks.

From Ransomware to Extortionware: Security Threats Continue to Escalate

When ransomware first invaded networks via floppy disk in 1989, attackers sought payments of $500 from each of their 20,000 victims.

Today, Cybersecurity Ventures predicts that ransomware cost victims $20 billion in 2020, thanks to increasingly sophisticated tactics that infiltrate networks and inflict damage not only on individuals, but on corporations.[1]

To better recognize, respond to, and avoid ransomware, you need to understand how it's evolved and where you can turn for help.

Attackers now employ multiple tactics to gain access to your network.
Not only do they rely on phishing, pop-ups, and messaging platforms, but now they get entry from initial access brokers to monetize larger compromises.

Double attacks on data hamstring access to both your data and your privacy.
Rather than just demand payment to decrypt data, attackers exfiltrate it before they decrypt it—potentially leaving confidential data vulnerable, even if you have a backup.

Demands for ransom have gone social.
Companies now face pressure to pay or risk disclosure of compromising or damaging information to public audiences.

Today's ransomware has escalated to extortion. To combat it, our approaches to these evolving threats must change.

- **Presidio partners with SentinelOne in using their One platform to prevent, detect, respond, and hunt in the context of all enterprise assets.**

Each of the following can be a vector of infection for ransomware attacks:

1. Phishing
2. Compromised websites
3. Malvertising
4. Exploit kits
5. Downloads
6. Messaging applications
7. Brute force via RDP

[1] Morgan S, Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021, *CyberCrime Magazine*, October 2019.

Moving to the Cloud: Protect Yourself at Every Altitude

Migrating critical workloads to the cloud may help free up space and transform your digital environment, but does it safeguard you from ransomware attacks?

Unfortunately, the answer is no.

When you update your files locally, they synchronize to cloud storage. As ransomware starts encrypting files locally, this action appears as a change in files—triggering a synchronization in the cloud. Therefore, it's possible for a **single end user infected with ransomware** to inadvertently introduce ransomware-encrypted files to the cloud—holding your enterprise data hostage.

▶ **With Presidio and SentinelOne, your off-premises workloads remain protected.**

SentinelOne Ransomware Protection Features

ROLLBACK

Saves and protects shadow copies of files, helping you quickly recover from a ransomware infection.

REAL-TIME BEHAVIORAL PROTECTION

Software provides broad visibility into endpoints and can then predict advanced or hidden ransomware attacks based on execution behavior.

KERNEL-SPACE OPERATION

Operates in kernel mode, most generally reserved for the lowest-level, most trusted functions of the operating system.

PREDICTIVE EXECUTION INSPECTION

Monitors all suspicious software, including memory- and script-based ransomware, to better understand its behavior.

AUTOMATIC RESPONSE AND MITIGATION

As threats emerge, the One platform allows for automatic response and mitigation of ransomware in real time.

BROAD PLATFORM SUPPORT

Supports Mac OS X, iOS, and Android devices. The One platform also supports virtual environments like Linux.

191 days

The average time cybercriminals spend inside a network before being discovered.[2]

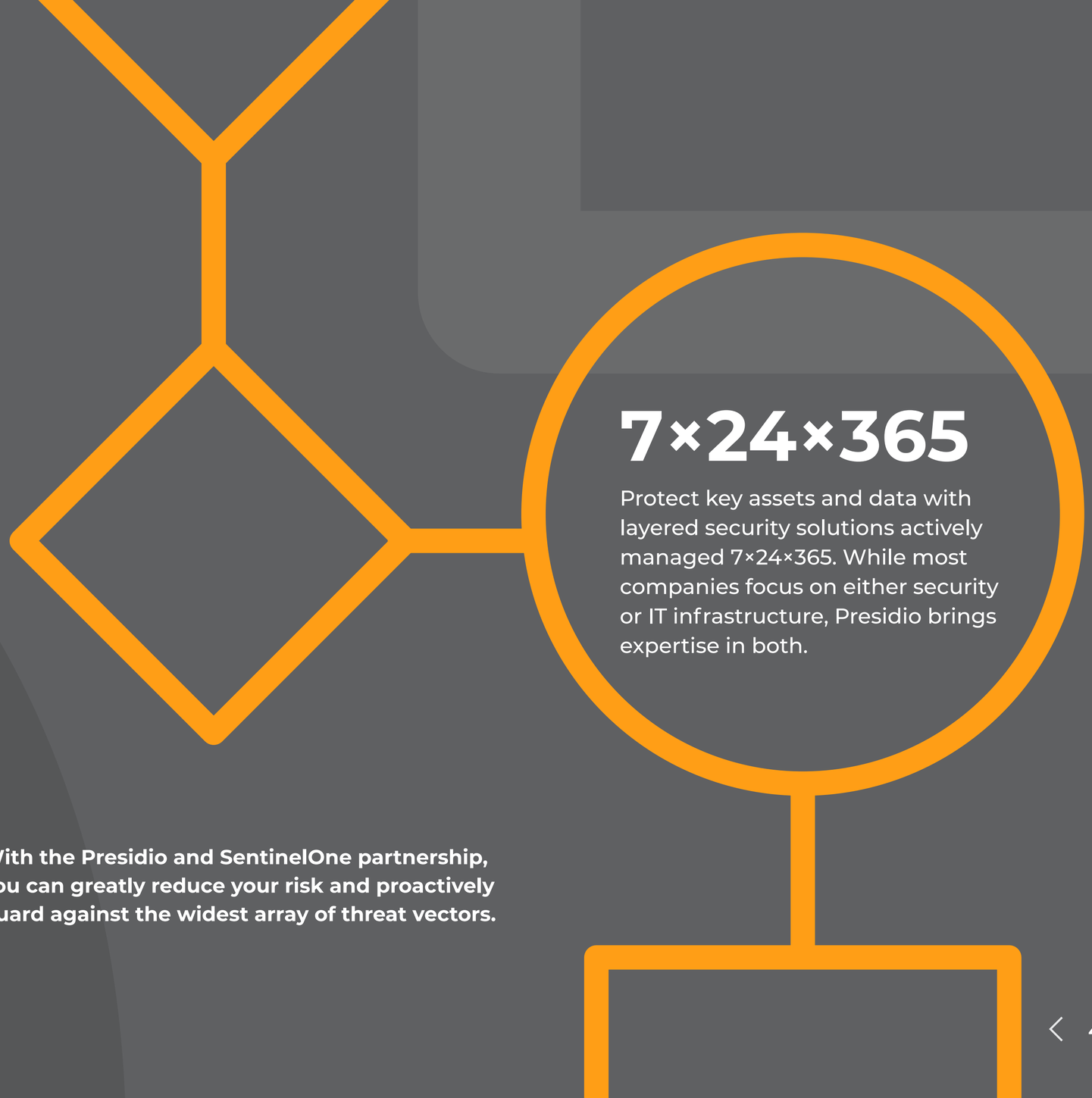
You can't watch what happens in the cloud all the time, but Presidio can. We've got the tools and expertise to monitor and manage threats, spanning from **24/7 Level 1 monitoring/triage to Level 2 application and data support.**

[2]Chheda R, "Six Steps to Successful and Efficient Threat Hunting," SentinelOne whitepaper, January 2021.

Locked Up in Jail, Your Data Can Still Be Exposed to the General Population

At one time, companies exchanged ransom payments to decrypt locked data and gain access to valuable files. Today, attackers aren't only interested in holding your data captive—they maliciously export it before they encrypt it, leaving your organization doubly vulnerable. Even if you can retrieve backup data, you may still have to pay—or face exposure.

- Presidio uses SentinelOne's multiple patented artificial intelligence (AI) algorithms to protect against the widest array of ransomware.
- Presidio manages, detects, and responds to threats that may show up on endpoints.
- Together, Presidio and SentinelOne eliminate dependency on connectivity, cloud latency, and human intervention. On-device AI prevents known and unknown threats in real time.
- SentinelOne enables devices to self-defend and heal themselves by stopping processes, quarantining, remediating, and even rolling back events to keep endpoints in a perpetually clean state.



With the Presidio and SentinelOne partnership, you can greatly reduce your risk and proactively guard against the widest array of threat vectors.

Hard to Recognize, Ransomware Assumes a Brilliant Disguise

Securing your network can feel like extinguishing the flames of a fire, while looking out for other signs of smoke nearby. Even after you are successful at stopping an attack, your team must always stay on lookout for emerging bad actors employing new tactics and techniques.

You don't have to face this battle alone.

SentinelOne is equipped to undertake "threat hunting," or the process of searching across networks and endpoints to identify threats that evade security controls before they can execute an attack or fulfill their goals.

A proactive approach to finding threats hidden in your network, this process involves formulating hypotheses on the existence of potential threats, which are then either confirmed or disproven based on collected data and analysis.

- **Together, Presidio and SentinelOne facilitate faster responses and more sophisticated threat hunting that reveals the most elusive and deceptive ransomware.**

38%

of advanced, emerging threats are missed by traditional security tools, according to a report published by Cybersecurity Insiders.[3]

Six Steps

to Successful and Efficient Threat Hunting

1. Capture the right data.
2. Understand your baseline environment.
3. Develop a hypothesis.
4. Investigate and analyze potential threats.
5. Rapidly respond to remediate threats.
6. Enrich and automate for future threats.[4]

[3] Cybersecurity Insiders, "The Importance of Threat Hunting Automation for XDR," 2020.
[4] Chheda R, "Six Steps to Successful and Efficient Threat Hunting," SentinelOne whitepaper, January 2021.

Ignoring Your Gaps Can Result in Devastating Losses

Protecting your network against ransomware isn't a one-time fix, nor is it restricted to one part of your network. Most organizations lack the deep expertise needed to recognize gaps in their end-to-end security in real time—and over time.

The evolving connection of laptops, tablets, mobile phones, Internet of things devices, and other wireless devices to corporate networks continues to create ample pathways for ransomware threats.

How Can You Keep Up?

Presidio and SentinelOne can help you mind the gaps in security—today and tomorrow.

A recent Gartner Peer Insights review gave SentinelOne 4.9 stars out of 5.0 stars for its Endpoint Protection Platform, with 97% of reviewers recommending it for performance impact on endpoint, cloud management, prevention, and ease of use, among others.[5]

And, should your company experience an attack, SentinelOne has a Ransomware Warranty that ensures no ransomware attack goes undetected and causes irreparable damage—giving you the security of financial protection in the event of ransomware attacks on your network.

- **In addition to administering SentinelOne, Presidio offers services and solutions that complement your team. From managed security to a federated service model and remote workforce management, our experts can help free up your experts to focus on innovation while we keep you protected.**

$1,000
per endpoint

$1 million
per company

SentinelOne's cyber threat protection warranty program provides its customers with financial support of $1,000 per endpoint, or up to $1 million per company, securing them against the financial implications of a ransomware attack, if the company indeed suffers an attack and SentinelOne is unable to block or remediate the effects.

[5] SentinelOne Endpoint Protection Platform Reviews, Gartner Peer Insights report, 2019.

Experience Enterprise Security with Presidio

Presidio can help support the lifecycle of your business. With deep expertise across data, applications, infrastructure, user experience, and operations, our experts are thinkers AND doers, focused on accelerating time to outcome for our customers.

To keep your network protected from all threats, Presidio offers security assessments that evaluate the strength of your infrastructure over time. No matter what sector you do business in, Presidio can help you analyze your IT ecosystem, identify products and solutions, and administer operational support today and in the future.

Presidio Expertise

5,000+
security clients across every major vertical

500+
public cloud certifications

1,600+
engineers across the nation

4:1
engineer-to-account manager ratio

400+
managed services engineers

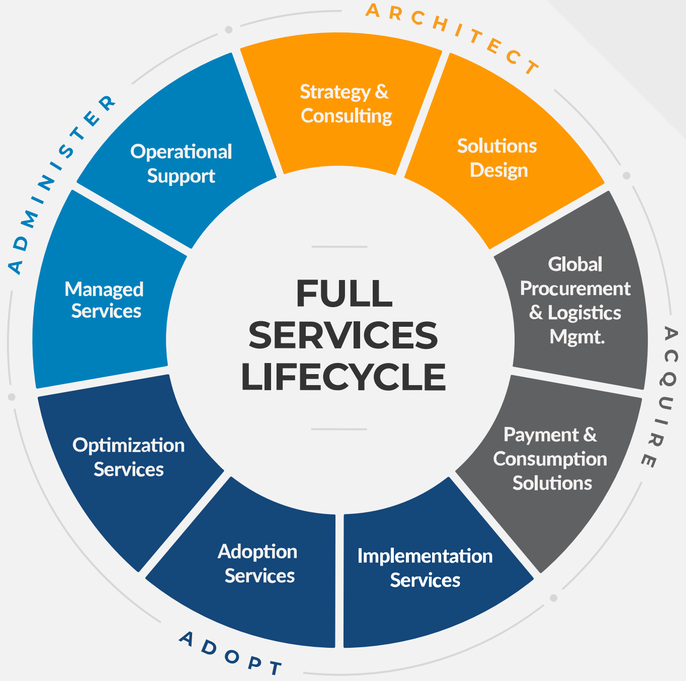
156+
countries that Presidio does business in

1,000+
private cloud certifications

60+
global offices including offshore service capabilities

Presidio Security Assessment

Driven by the industry standard NIST Framework methodology, our assessment measures your security maturity and gathers stakeholders from every IT discipline to illustrate a 360-degree actionable view of your cybersecurity landscape.



Stronger Together: Presidio and SentinelOne

With Presidio and SentinelOne, you can experience the joint benefits of:

- Constant monitoring of your endpoints
- Automation and immediate response to ransomware threats
- Cloud-delivered solutions
- Detection of threats before traditional security controls identify them

Stay connected with us.

About Presidio

Presidio is a leading North American digital systems integrator focused on digital infrastructure, cloud, and security services solutions. We deliver this technology expertise through a full lifecycle model that encompasses consulting, implementation, and design.

By understanding how our clients define success, we help them take advantage of the latest technology advances, simplify IT complexity, and optimize their environments today while enabling future applications, user experiences, and revenue models.

Presidio Managed Detection and Response Services provide a holistic approach to attaining a cybersecurity posture that can help meet risk management objectives and reduce the burden of spiraling threats.

LEARN MORE

We partner with proven technology leaders with best-of-breed digital business transformation tools to provide world-class, cloud-ready, secure, agile, and modern infrastructure application and data solutions.

About SentinelOne

SentinelOne is shaping the future of endpoint security with an integrated platform that unifies the detection, prevention, and remediation of threats initiated by nation states, terrorists, and organized crime.

SentinelOne's unique approach is based on deep inspection of all system processes combined with innovative machine learning to quickly isolate malicious behaviors, protecting devices against advanced, targeted threats in real time.

SentinelOne was formed by an elite team of cyber security and defense experts from IBM, Intel, Check Point Software Technologies, McAfee, Palo Alto Networks, and the Israel Defense Forces.

LEARN MORE

Defend Against Ransomware with Presidio

Are you ready to detect the latest threat? See how your security stacks up by taking a Presidio Security Assessment.

GET STARTED