Progent™

SentinelOne Certified Partner

Ransomware Endpoint Detection and Response (EDR)

Progent's ransomware defense services: AI and machine learning-based protection plus rapid recovery and root-cause forensic analysis

Ransomware can cripple or kill a company. Progent offers services that combine advanced technology and the skills of cybersecurity experts to assist organizations of any size to respond effectively to crypto-ransomware attacks. Progent's services include enterprise-wide preparedness reports, 24x7 monitoring, threat detection based on AI and machine learning (AI/ML), and fast restoration of network operations led by Progent's veteran team of mitigation consultants.

Progent's ransomware defense solutions are built both to stop ransomware assaults before they stop your business and to restore compromised networks to productive operation as quickly as possible. Progent's ransomware defense services can be delivered online to save time and expense. Progent has experience working with top cyber insurance companies like Chubb to perform preparedness audits, 24x7 monitoring, fast cleanup, settlement negotiation, and root-cause forensic analysis.

Services for Ransomware Defense, Incident Response, Recovery, and Forensics

Progent offers a range of subscription services and emergency response support to help your business counter ransomware attacks. Services cover filtering, detection, containment, and cleanup:

- *Ransomware Vulnerability Assessment Report* is based on an online interview with a Progent security expert. The report includes recommendations for creating your security and backup solution so you can more efficiently block or recover from a crypto-ransomware assault
- 24x7 protection for Windows, macOS, Linux, iOS and Android endpoints. This subscription service uses SentinelOne AI/ML technology to guard local and cloud resources and provides a unified platform to manage the entire threat lifecycle including filtering, detection, containment, cleanup, and forensics.
- Restore an IT network damaged by a ransomware attack. Recovery teams include relevant subject matter experts (SMEs) and will work round the clock to put critical IT services back online ASAP.
- Progent's experienced ransomware negotiation experts can assist your business to reach a settlement agreement with ransomware threat actors (TAs) after an assault by a ransomware variant such as Ryuk, Maze, Sodinokibi, DopplePaymer, Conti or Nephilim.
- Progent's ransomware forensics consultants can preserve the evidence of a ransomware attack and perform a detailed root-cause forensics analysis without interfering with the recovery process.

Ransomware 24x7 Hot Line: Call 800-462-8800

Progent's **Ransomware 24x7 Hot Line** is designed to guide organizations to carry out the urgent first phase in responding to a ransomware assault by stopping the bleeding. Progent's remote ransomware engineer can assist businesses to identify and isolate breached servers and endpoints and protect clean assets from being compromised. If your network has been penetrated by any strain of ransomware, don't panic. Get help quickly by calling Progent's **Ransomware Hot Line** at **800-462-8800**.

Progent's Qualifications

Progent has delivered remote and on-premises network services throughout the United States for more than 20 years and has been awarded Microsoft's Gold Partner certification in the Datacenter and Cloud Productivity competencies. Progent's team of SMEs includes professionals who have earned advanced certifications in foundation technology platforms including Cisco infrastructure, VMware virtualization, and major Linux distros. Progent's cybersecurity consultants have earned top certifications including CISM, CISSP-ISSAP, and CRISC. Progent also offers top-tier support in financial and ERP applications.

This scope of expertise allows Progent to salvage and integrate the surviving pieces of your network after a ransomware attack and rebuild them rapidly into a functioning system. Progent has collaborated with top insurance providers like Chubb to help businesses clean up after ransomware assaults.

Find Out More About Progent's Ransomware Detection and Response Services

To learn more about Progent's support services for ransomware protection, recovery, and forensics, call **800-993-9400** or send email to **information@progent.com**

SERVICES

- **Vulnerability Assessment**
  Report evaluates your ability to survive a ransomware attack and suggests enhancements to block or recover from a breach.
- **24x7 RMM Threat Protection**
  Progent's Remote Monitoring & Management services provide non-stop protection for onsite and cloud resources.
- **Advanced Heuristics**
  Replaces legacy AV products based on signature matching with AI/machine learning from SentinelOne to block zero-day threats including new strains of ransomware.
- **Optimal Recovery Teams**
  Ransomware recovery teams have skill sets that match the compromised system and are staffed to provide round-the-clock restoration services.
- **Settlement Negotiation**
  When required, Progent can provide the help of experienced settlement negotiators to deal with ransomware threat actors.
- **Forensics**
  Progent can carry out root-cause forensics in parallel with network restoration services for fast recovery.

WHY PROGENT?

- **Security Expertise**
  Progent's experts have earned CISM, CISSP-ISSAP, GISA and CRISC security certs.
- **Endpoint Integration**
  Progent offers expertise in all popular endpoints: Windows, Linux, macOS, iOS, Android.
- **Virtualization Expertise**
  Progent offers the help of experts certified to support Hyper-V, VMware, and Citrix.

■ Headquarters: 2570 N. First Street, 2nd Floor, San Jose, CA 95131
■ Email: information@progent.com ■ Web: www.progent.com ■ Phone: 800-993-9400 ■ Fax: 800-325-5300
P/N 220326B