Dentistry Under Attack

5 Critical Steps for Preventing Ransomware in Dentistry

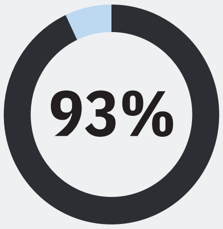
The Rise of Ransomware

The explosion of ransomware attacks aimed at hospitals, clinics, and private practices does more than just compromise patient data and the systems and medical devices used to drive patient care—it also endangers patients' lives!

24.1 million

The U.S. Department of Health and Human Services found that ransomware was the cause of roughly 50% of healthcare data breaches in 2020. Consequently, the records of 24.1 million patients were released to unauthorized parties, according to the report.

Sophos reported a **94% increase** in ransomware attacks.



Don't think it can't happen to you. According to the Herjavec Group, 93% of healthcare organizations have experienced a data breach of some kind during the last three years. And in 2019, the healthcare industry **lost $25 billion** to ransomware attacks, SafeAtLast reported.

Ransomware attacks are more targeted and sophisticated than ever before. It's critically important to have a partner who is an extension of your team to help you keep pace with the ever-changing threat landscape and bolster your cybersecurity defenses.

We can help! Contact us today to learn more.

Siligent LLC
8022102763
https://www.siligent.com
316 Charbonneau Dr,
SAINT ALBANS, VT 05478

5 Critical Steps for Ransomware Prevention and Mitigation

1.Discover & monitor every asset

Asset discovery featuring automated network scans is an important service. With ongoing scans, you can quickly find and monitor new devices as they join the network and understand each device's health.

2.Software patching

A remote monitoring and management (RMM) tool helps with continuous patching, enabling you to automatically deploy updates to endpoints and ensuring your patching never falls behind. You should also be sure that your anti-virus and anti-malware solutions are set to automatically update and run regular scans.

3.Regular data backups

Integrated backup and disaster recovery (BDR) solutions provide more streamlined service management with far less chaos. It's also crucial to secure your backups. Make sure they are not connected to the computers and networks they are backing up or else they could become infected in the event of a ransomware attack.

4.Deploy an endpoint protection tool

Endpoint detection and response (EDR) solutions help protect endpoints such as servers, laptops, desktops, mobile devices, and more to quickly identify malicious activity, as well as automatically taking remediation actions such as restoring unsafe files to an acceptable previous state.

5.Enhancing your cybersecurity toolset

When it comes to cybersecurity, there is no such thing as too secure. Here are a few examples of tools and services you should consider adding to your cybersecurity tech stack:

- ✓ Risk assessment software
- ✓ Email monitoring
- ✓ Security information & event management (SIEM)
- ✓ Threat intelligence feeds

SILIGENT Intelligent Technology