Don't Ignore the Threat of Ransomware

This Deadly Virus Will Attack a Business Every 14 Seconds in the Next Year[1]

It's the worst kind of malware there is. Ransomware holds your systems or data hostage until a large sum of money is paid. You need only click on an infected link once for cybercriminals to deliver a virus that will put you out of business. Today, the increasing sophistication and frequency of attacks make ransomware one of the most significant threats your enterprise could face.

Ransomware Attacks on the Rise

Attackers are persistent and clever, continually evolving new ways to defeat cybersecurity measures.

- **$11.5 billion in damages** caused by ransomware over the last two years[1]
- **$133,000 in average costs** per ransomware attack in 2017[1]
- **54% of organizations** do not have specific anti-ransomware protection in place[2]
- **77% of organizations** infected with ransomware were running up-to-date endpoint protection[3]

Increased Connectivity Brings Security Challenges

The number of connected devices in the world is constantly expanding, so even more of your crucial business data and apps will be exposed and vulnerable.

- **100X more data** will be stored in the cloud by 2022[4]
- **6 billion more** smartphone devices will be added in the next four years[4]
- **50 billion devices** will be connected to the internet by 2020[4]

Ransom Isn't the Only Thing You'll Pay

A ransomware attack can also cost you money in lost productivity, idle employees, and missed revenue opportunities.

- **89% increase** in the cost of the average ransom in 2019[5]
- Up to **10X the actual ransom amount** is suffered in downtime costs[4]
- **7.3 days lost on average** during ransomware attacks[4]
- **$64,645 average cost** of ransomware related downtime[4]

A 3-Layer Defense Strategy

The best defense against ransomware is multilayered. It begins with strong anti-ransomware protection and extends to retrieval of lost data and restoring systems from the most recent backups.

- **Prevention** - Protect critical systems and data
- **Remediation** - Retrieve data to be functional again
- **Restoration** - Bring systems back to original state

Protect Your Data When Prevention Fails

Backup is essential for safeguarding your data in the event of an attack. The best backup, recovery, and restoration solutions work fast to minimize downtime and are easy to use. For example, StorageCraft® ShadowXafe® is a next-generation data protection solution that offers true, one-click disaster recovery as a service. It allows you to recover data instantly from booted backup images, so files are restored in seconds, and entire systems are restored in minutes.

Placeholder for partner's value proposition

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin eu velit aliquet, viverra arcu ac, ullamcorper lorem. Duis vel arcu blandit justo porta scelerisque. Phasellus tristique mi vel mattis posuere. Proin dictum nunc sit amet velit iaculis tempor. Suspendisse potenti. Sed porta rutrum est. Mauris quis tellus hendrerit sem faucibus cursus. Aenean congue est ipsum, sed euismod lectus hendrerit nec. Donec non feugiat libero. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin eu velit aliquet, viverra arcu ac, ullamcorper lorem. Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Contact [INSERT PARTNER NAME] at [INSERT PARTNER CONTACT INFO] to learn more about advanced data protection solutions.

[1] "Ransomware Damage Report" Cybersecurity Ventures, 2017.
[2] The State of Endpoint Security Today. Accessed April 22, 2019.
[3] Understanding ransomware and the impact of repeated attacks, Accessed April 22, 2019.
[4] Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac" https://cybersecurityventures.com/cybersecurity-almanac-2019
[5] "Ransom amounts rise 90% in Q1 as Ryuk increases" Coveware, 2019.