Enhancing Cyber Insurance with Ransomware Protection

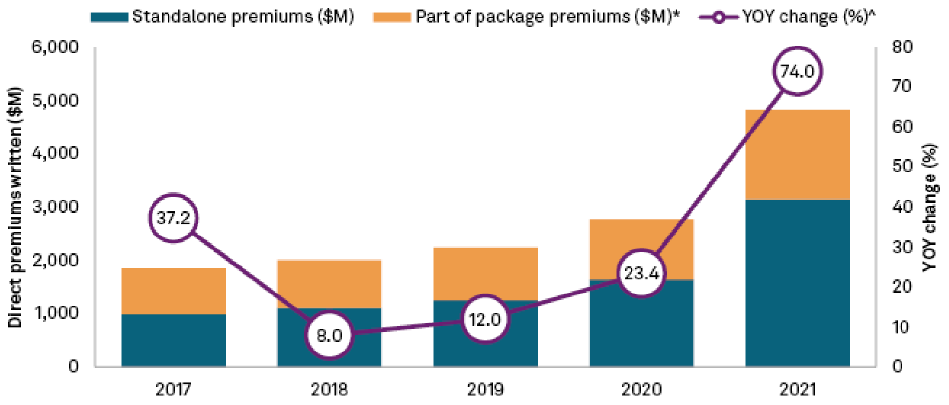
By David Cerf, Chief Data Evangelist at GRAU Data

Growing Threat of Cyberattacks

The prevalence and impact of cyberattacks have reached alarming levels. McKinsey's projection of $10.5 trillion in annual damage by 2025 highlights the urgency of addressing the escalating cyber threat landscape. A survey of midsized companies suggests that threat volumes almost doubled from 2021 to 2022. Furthermore, the emergence of unseen threat groups and malware underscores the need for more robust security measures.

The Rise of Cyber Insurance

Total US cyber insurance premiums soar 74% in 2021



Data compiled June 30, 2022.
* Includes both quantified and estimated direct premiums written.
^ Value shown is based off of the year-over-year change of total cyber insurance direct premiums written.
Data reflects the aggregation of all individual property and casualty filers that submit regulatory statements to the NAIC.
Based on direct premiums written reported within annual NAIC statutory property and casualty filings: Cybersecurity and Identity Theft Insurance Coverage Supplement Part 2 – Stand-Alone Policies and Part 3 – Part of a Package Policy. U.S. filers only but may include business written outside the U.S.
Source: S&P Global Market Intelligence

To protect themselves from the financial and reputational fallout of cyberattacks, businesses are turning to cyber insurance. High-profile incidents like the Colonial Pipeline ransomware attack have increased demand for cyber insurance in recent years. In 2021 alone, direct written cyber insurance premiums increased by an impressive 74%.
According to a report from the CyberEdge Group, 86.2% of U.S. organizations experienced at least one cyberattack in 2021, marking an increase from the previous year. The alarming rise in cyberattacks emphasizes the urgent need for robust cybersecurity measures and comprehensive cyber insurance coverage.

Stricter Coverage Standards

Insurers are implementing stricter coverage standards in response to the escalating cyber threat landscape. They encompass various measures, including the enhancement of basic authentication and authorization controls through multifactor authentication and least-privilege access models. By aligning with these industry best practices and meeting the heightened standards set by insurers, businesses can significantly enhance their cybersecurity posture and mitigate potential risks.

Impact on SMB

A single ransomware attack can have catastrophic consequences, potentially leading to the downfall of an entire enterprise. When it comes to cybersecurity, small and midsize businesses (SMBs) and midmarket companies encounter distinct challenges. What may be a minor breach for a large enterprise can prove devastating for smaller entities.

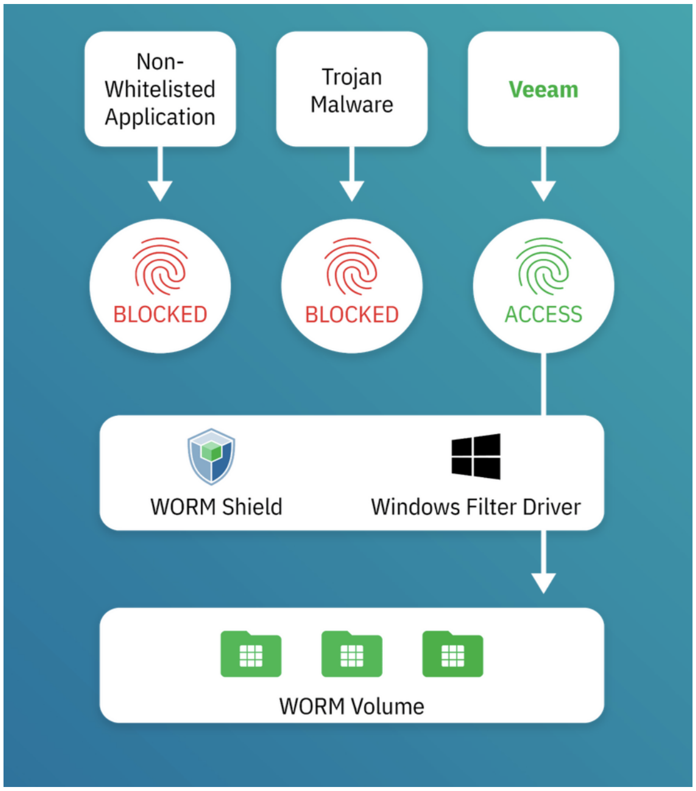
To exemplify the gravity of ransomware attacks on SMBs and midmarket companies, consider the case of a midsize steel structure manufacturer based in Texas. In May 2019, this company was pushed into bankruptcy due to a ransomware incident that permanently encrypted critical tooling and financial accounting software. Unfortunately, they could not recover their backup data. Moreover, the aftermath of a breach can inflict irreparable harm to customer trust. Astonishingly, nearly 10 percent of respondents in the McKinsey study disclosed terminating business relationships with suppliers upon discovering a data breach.

Fortifying Cybersecurity Defenses Against Ransomware

In the realm of cybersecurity and cyber insurance, safeguarding against ransomware attacks stands as a critical imperative. The persistent and formidable nature of ransomware poses an ever-present threat to businesses, rendering traditional security solutions and data backups inadequate. In order to establish an impregnable defense, a paradigm shift is necessary, wherein backup repositories are fortified with cutting-edge technologies such as Blocky for Veeam. Blocky enhances protective measures and strengthens resilience against the dangers of ransomware.

Blocky is a powerful addition to Veeam that provides the ultimate defense in ransomware protection for backup data. By leveraging Windows filter driver technology, Blocky transforms the Veeam backup repository into a WORM (write once, read many). This unique approach creates maximum protection against the corruption caused by ransomware attacks. Only authorized and trusted Veeam processes are granted exclusive access to modify or delete data, ensuring the integrity and availability of critical backup information. Additionally, Blocky's innovative fingerprint technology assigns unique identifiers to authorized processes, further reinforcing the security of the backup data and preventing unauthorized modifications.

Resilient Recovery: Safeguarding Business Continuity Against Ransomware with Blocky-Enhanced Backup Solutions



By incorporating the cutting-edge technology of Blocky, organizations can enhance their ability to swiftly recover from ransomware attacks and withstand extortion attempts by implementing a resilient and secure backup system. By leveraging the comprehensive capabilities of Blocky, organizations effectively safeguard the integrity and availability of critical data, allowing them to restore their backup systems and resume normal operations with minimal disruption, even in the event of malware infecting the network and backup servers.

Key Features of Blocky for Veeam

Blocky offers a range of key features that make it an essential tool for enhancing cybersecurity and cyber insurance coverage:

1. WORM Architecture and Fingerprint Technology: Blocky's WORM architecture ensures that backup data remains immutable, preventing ransomware from modifying or encrypting the information. The integration of fingerprint technology assigns unique identifiers to authorized Veeam processes, further securing the backup data.

2. Exclusive Access for Authorized Veeam Processes: Blocky grants exclusive access rights to approved Veeam processes, effectively blocking unauthorized processes from tampering with or compromising the backup data. This ensures that only trusted components can modify the repository.

3. Event Monitoring and Reporting Capabilities: Blocky provides Veeam administrators with comprehensive event monitoring and reporting capabilities. This enables prompt detection of potential threats or anomalies, allowing for proactive response measures to be implemented swiftly.

4. Seamless Integration and Easy Deployment: Blocky seamlessly integrates with the existing Windows backup server infrastructure, eliminating the need for additional hardware or complex Linux integration. The installation process is straightforward, enabling swift deployment within the Veeam environment without compromising security or operational efficiency.

With Blocky for Veeam, organizations can fortify their Veeam backup data against the relentless onslaught of ransomware attacks. By implementing this solution, businesses enhance their overall cybersecurity posture and bolster their cyber insurance coverage.

Conclusion

In an increasingly digital world, the threat of cyberattacks continues to rise. However, securing adequate cyber insurance coverage is becoming more challenging due to the evolving threat landscape.

To navigate these challenges effectively, implementing advanced technologies like Blocky for Veeam can provide the maximum ransomware protection, fortify backup data, and enhance overall cybersecurity resilience.

Sources:

1. *New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers, October 27, 2022 | McKinsey & CO - https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers*
2. *Insurers revisit cyber coverage as demand, premiums spike, S&P Global Market Intelligence July 22, 2022 - https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/insurers-revisit-cyber-coverage-as-demand-premiums-spike-70880071*