Commvault

eBOOK

Out of sight, NOT out of mind: why endpoint protection is critical to your cyber resilience

Considerations for your Endpoint Data Protection
in an era of remote work

Introduction

Many IT professionals place their focus to grow cyber resilience and data centers, but they are leaving one area wide open for attackers to disrupt the business—endpoints. These devices are responsible for 70% of breaches so they are definitely not out of mind when a malware attack hits the business.[1]

And it's no secret that cyberattacks continue to rise. Not only are they rising—they are changing.

- There has been a 224% increase in a category called hack tools. These hack tools are programs that can probe through systems and networks and download malicious payloads.[2]
- Fileless malware, where attack codes live only in RAM and do not write files to disk, grew 256% over the first half of 2019.[2]
- Web skimmers, which inject code on the server or sometimes the client side of online transactions to harvest credit card numbers, grew 187%.[2]

ENDPOINT PROTECTION—THE GAP IN MANY CYBER RESILIENCE STRATEGIES

With so many malicious programs out there, it is imperative that security is in place for all potential entry points to your network. 94% of malware is still delivered via e-mail.[2] That's a staggering number! Since laptops and desktops are the starting point for many of these e-mail originated attacks, they are definitely not out of mind when your company is affected.

ENDPOINTS ARE FUNDAMENTAL TO RUNNING YOUR BUSINESS

Although applications are moving to the cloud, accessing the application still requires some type of endpoint device. That means all the data transactions that occur from the endpoint to the server can potentially be at risk. Endpoint security can help regulate data traffic, monitoring incoming and outgoing traffic for sensitive data that should not leave your enterprise.[3]

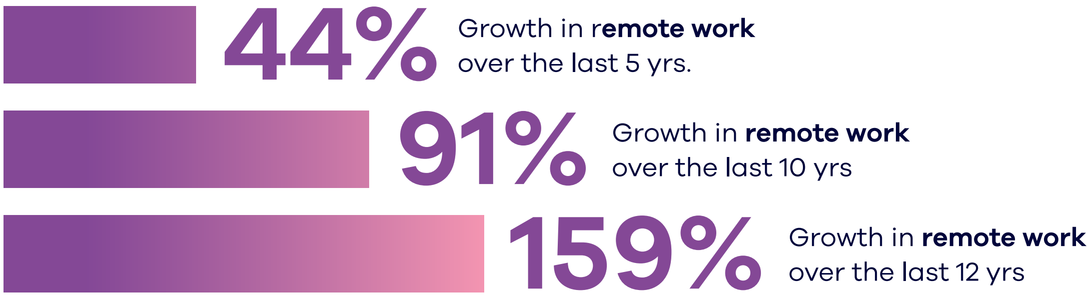
YET SOME STILL DO NOT HAVE AN ENDPOINT SECURITY STRATEGY IN PLACE

Surprisingly, there are still some businesses that have not incorporated endpoint security in their overall cyber resilience strategies. According to a recent poll, 49% responded that endpoint security is nonexistent in their organization.[4]

AND THE NUMBER OF REMOTE WORKERS CONTINUE TO CLIMB

The growth of remote workers significantly expands the footprint of devices that are prone to attack.

Trends in Remote Work Growth



Remote Work Statistics: Shifting Norms and Expectations, Feb 13, 2020

IF YOUR ENDPOINTS ARE COMPROMISED, YOU NEED TO BE PREPARED

The good news is that there are solutions available that can help. To cover all facets of your endpoint security, it's important to take a comprehensive approach that includes endpoint backup and recovery. While detection and prevention are critical, ensuring endpoint data is backed up and having a plan in place to recover data should malware penetrate your defenses is equally as important.

AND THERE ARE REAL BENEFITS FROM PROTECTING ENDPOINTS

Overall, backing up your business' data can shorten the ramp when data has been disrupted, whether the disruption was a natural disaster or a cyber attack.

Endpoint backup and recovery should be comprehensive but not intrusive to keep the business moving while protecting your valuable data. Protection begins with secure data transmissions and security of the device itself. For example, the ability to detect abnormal file access lets you know when something may be wrong. You can minimize impact to user productivity with automated backups that silently backup your data without the need for user intervention. Characteristics such as source side deduplication along with transmitting only incremental or changed data from previous backup ensures no noticeable impact to user productivity.

DON'T COMPROMISE ON FEATURES WHEN PROTECTING YOUR ENDPOINT DEVICES

In a recent survey, 46.8% of respondents said they wanted real-time endpoint and application visibility. 32.7% of those respondents also said their biggest challenge would be the complexity of deploying, managing and using endpoint solutions.[3]

Consider This

Solutions that include endpoints must be fundamental to any cybersecurity strategy, particularly as the workforce becomes more mobile. A Ponemon Institute study reveals 68% of IT security professionals say their company experiences one or more endpoint attacks that compromised data assets or IT infrastructure in 2019, an increase from 54% of respondents in 2017. These attacks also inflicted more bottom-line business damage and impacted business continuity. Malicious actors and rogue software can lead to data loss and ransom demands which can prove to be very costly for organizations.

Organizations need to mitigate this risk of being held to ransom, by including data management and protection strategies in their overall endpoint security strategy.[5]

When choosing endpoint backup solution, you want to look for software that offers more than just an extra copy in the cloud or on an on-premises server.

- Automated backup and recovery: to minimize impact to user productivity
- Anomaly detection: Identify file access patterns deviating from the norm to catch risky and/or corrupted files before they get saved to your backup location
- Remote wipe: particularly useful when you have a mobile workforce
- Air gapped copy: keep a separate data copy away from the affected source location
- Deduplication: to optimize bandwidth and network usage—particularly when supporting large numbers of remote workers
- Scalability: to ensure the solution can grow with your business
- Rapid Recovery: restore your data more easily and utilize point-in-time, granular restores and metadata search capabilities
- Secure data transactions: using two-factor authentication or SSO with SAML
- Secure data transmissions: best in class encryption of data at rest and in flight
- Unlimited storage: to keep up with content volumes as they continue to grow over time

Consider This

Look beyond simply creating duplicate files. Include capabilities that proactively flag abnormal actions, minimize impact to productivity, meet strict security requirements and scale to grow with your business.

COMMVAULT CLOUD BACKUP & RECOVERY FOR ENDPOINTS.

At Commvault, our engineers and product teams have decades of combined experience protecting customer data. Our cyber resilience platform is powered by Metallic AI delivering industry-leading data protection capabilities with security best practices and advanced insights baked in.

Commvault Cloud Backup & Recovery for Endpoints uses industy-leading backup and recovery expertise for the hybrid enterprise to protect laptops and desktops whether they run on Windows, Linux or Mac operating systems. Minimize network usage with source-side deduplication and "incremental forever" file updates, all through an SSO with SAML secure communication channel. And manage your endpoints using reporting and alerting functionality while leveraging the simplicity and ease of use of SaaS.

So when you are looking for the best solution for your endpoint data protection, consider the expertise and rich feature set of Commvault Cloud Backup & Recovery for Endpoints.

[1] What is Endpoint Security Today? Big Data and Mobile Trends Point to the 'Startpoint', April 16, 2019
[2] Top cybersecurity facts, figures and statistics for 2020, March 9, 2020
[3] Here is Why Endpoint Security is Important For Your Enterprise, Oct 2, 2019
[4] The State of Endpoint Security Management in 2022: It's Worse Than You Suspect, 2022
[5] Ponemon Institute, Study on the State of Endpoint Security Risk, 2020, n=671, Jan 2020

To learn more, visit **commvault.com/free-trial**