Exosphere

Endpoint Protection

"Protect Your Endpoint,
Keep Your Business Safe."

White Paper

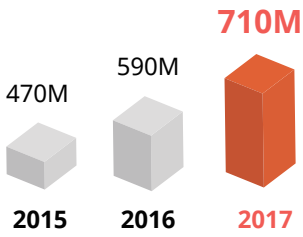
Exosphere, Inc.

getExosphere.com

Today's Threat Landscape

Cyber attacks today are increasingly sophisticated and widespread, rendering many security solutions, such as the traditional anti-virus, obsolete. Worse yet, such sophisticated cyber attacks in recent years are often financially motivated and result in data breaches. Such attacks no longer target only high-profile enterprises and government agencies, and small businesses too are becoming prime targets for cyber-criminals.

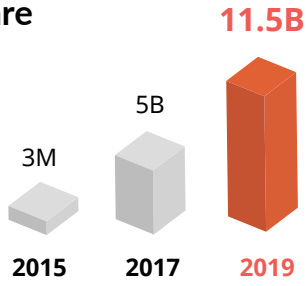
Total Malware



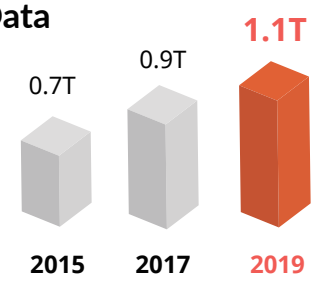
Crypto-Ransomware in 2017

*Ransomware Modifications

Cost of Ransomware Damage



Annual Cost of Data Breaches



Yet malware is just one of several attack vectors that account for the increasing breach incidents. Malware now includes new capabilities, such as Ransomware. And research shows that the insider threat and data loss are also critical threats that must be addressed.

Businesses need to get familiar with the slew of threats and vulnerabilities, some old and some emerging, and address them. The old anti-virus alone does not provide an adequate solution for to any of these threats.

Incidents by Type in 2017

Latest Patterns of Threats

Advanced Malware

Advanced malware is built for stealth and can slip through most legacy anti-virus solutions. Such malware often also includes sophisticated capabilities, such as command and control, data exfiltration, lateral movement and infection, and more. Legacy signature-based anti-virus is typically not capable of detecting or stopping advanced malware.

Data Loss

Data can be wiped out or corrupted as a result of malware, ransomware, human error or hardware failure. 140,000 hard drive crash every week in the US, causing serious loss of productivity.

Ransomware

In 2017 ransomware played a significant role in cyber attacks. Ransomware is a type of malicious code that limits the users from using their systems – typically by encrypting all their files, until the company pays a ransom in digital currency. WannaCry and Petya were two types of ransomware outbreaks that caused global panic over the past year.

Insider Threat

Insider threat presents an even more pervasive and serious threat than an external attacker. Rogue employees are likely to copy corporate data onto USB drives or forward it to unauthorized parties, putting your business at risk. And since we are talking about insiders, stopping this kind of threat is the most difficult.

Phishing

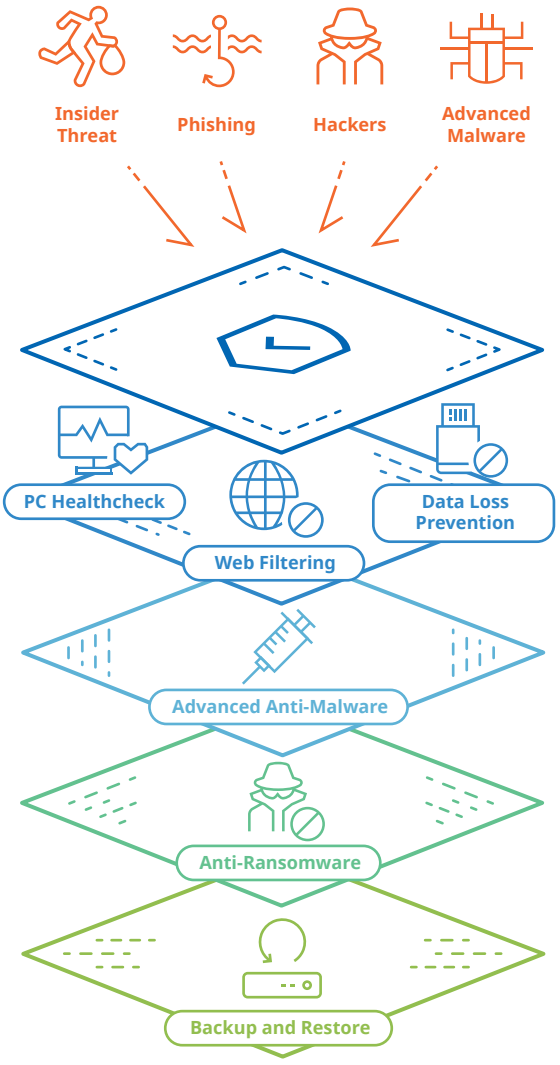
Phishing is the most common way to mount an attack, with over 90% of cyber attacks starting with a phishing email. Phishing typically starts with an email message fooling the user into entering his or her credentials into a web site or into running some malicious executable, and uses this as an entry point to retrieve user credentials and penetrate the organization.

PC Posture

Finally, one of the most important yet overlooked aspects of security is keeping up your PC's security posture. According to Gartner, less than 0.1% of cyber attacks will use a 0-day (unknown) vulnerability. In other words, patching known vulnerabilities in the operating system and critical applications can prevent 99.9% of attacks! Ensuring basic hygiene by updating the systems, ensuring the firewall and anti-malware tools are running, is therefore critical. Failure to do so often undermines all other security measures.

Exosphere™ Comprehensive Endpoint Protection Solution

The Exosphere endpoint protection agent offers simple, all-in-one coverage for all key attack vectors. It offers both breadth by protecting your business from multiple threats -- both external and internal, as well depth, by layering multiple types of protection. A single management console allows the administrator to manage all aspect of security, protecting both your PCs and your data. All this saves the cost and management overhead incurred if multiple security solutions are required, and allows small businesses with limited IT staff to enjoy a comprehensive solution.



Features of Exosphere

Advanced Anti-Malware

Exosphere scans files in real-time using an advanced anti-malware engine. The engine provides multi-layered detection, that applies signature-based, heuristics, and emulation methods. The Exosphere anti-malware engine updates quickly with threat intelligence collected from over 550 million endpoints.

Data Loss Prevention

Exosphere offers rich functionality to stop or deter insiders from sharing sensitive information. This includes discovering data on user's machines, blocking USB devices, file transfer sites, and adding watermarks to printed document.

Web Filtering

Filtering web sites is part of Exosphere's first line of defense. With a URL database of over 140 million web sites, Exosphere can prevent employees from visiting risky web sites that may contain malware or be used for phishing. The administrator may specify which of the 10 URL categories is allowed, thereby maximizing productivity and reducing risk.

Anti-Ransomware

Exosphere anti-ransomware protects your data by preventing untrusted applications and processes from accessing it. By doing so, malicious ransomware is prevented from to overwriting any files, even if it had infiltrated all other layers of defense.

PC Healthcheck

Approx. 0.1% of threats exploit an unknown vulnerability. Therefore, keeping your operating system and key applications up-to-date, and ensuring your configuration is correct is the best way to prevent your system from being compromised. Exosphere can scan your machines and automate the patching process for you, and verify your settings, thereby stopping any known threat.

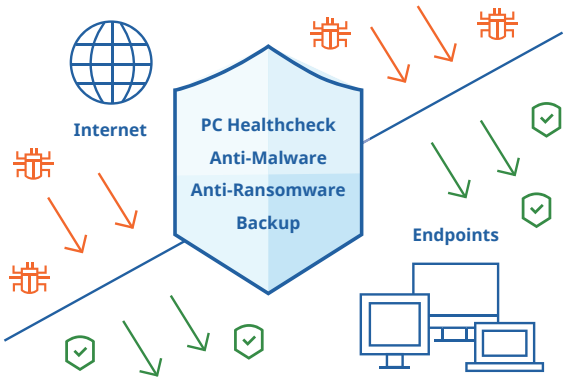
Backup and Restore

As a final layer of defense, Exosphere ensures your files are backed up at all times. Should ransomware or another malicious code infiltrate all other defenses, corrupted user data could be salvaged from backup. Backup repository is encrypted and de-duplicated to ensure efficiency and security.

Use Cases

Fighting Ransomware

The recent "WannaCry" ransomware outbreak in May infected over 230,000 computers in 150 countries. It was spread by exploiting a known Windows vulnerability. It then encrypted all PC files and requested ransom in Bitcoin to unlock all files.

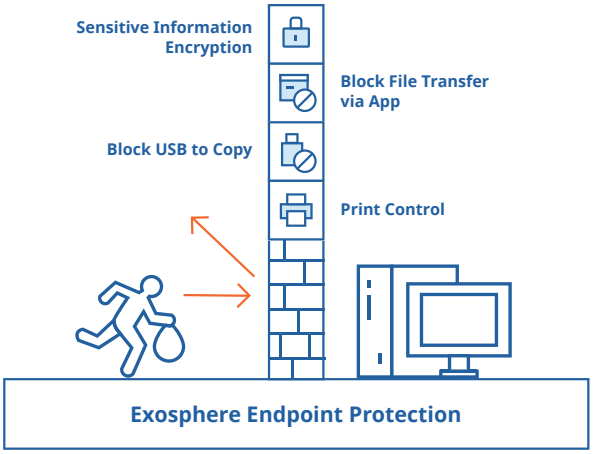


Exosphere's defense in depth is able to defeat such an attack:

PC Healthcheck	When PC Healtcheck is in place, the operating system is regularly patched, thereby WannaCry and other ransomware attempting to exploit known vulnerabilities will fail to spread.
Anti-Malware	Advanced anti-malware will neutralize the threat as soon as it is discovered in the wild.
Anti-Ransomware	Exosphere's anti-ransomware capability implements a data firewall that denies WannaCry (or any other unknown application) from overwriting user data.
Backup	Even if all else has failed and the ransomware was able to corrupt user files, these will easy to restore from the Exosphere backup.

Protecting Intellectual Property from Malicious Insiders

Tech companies have seen major leaks of their intellectual property in recent years. CAD files or product specifications have been leaked over USB devices, email, or via online cloud services.



Using Exosphere, it's easy to address this issue:

Discover and Secure Sensitive Data	Exosphere can scan all user devices to discover sensitive documents (e.g. CAD files, files containing credit card or social security numbers) and then generate a report, or even automatically encrypt such documents.
Block USB Devices	USB storage devices can be used to transfer large amounts of data outside the organization. Exosphere can apply Device Control policies that restrict the copying of files containing sensitive data (or all files) to USB devices. Such a policy can be assigned to all users or to specific groups of users (e.g. engineering). Exosphere may also be set to auto-encrypt any sensitive file moved to a USB device.

Block File Transfer	Files are often shared without permission over email, instant messenger or online services. Exosphere can be set to block file transfer via all these channels. Users may request exceptions from the administrator if they believe they have a legitimate business reason for it.
Deter Unauthorized Printing	Exosphere applies visible watermarks to printed documents. By doing so, the document will include the printer's information, thereby deterring the transfer of such a printout.

Summary

At the end of the day, what's ultimately most important to the business is to protect its data's privacy and its integrity. Addressing just a single threat, such as malware, is not sufficient. Trying to address each threat individually has a significant cost and requires considerable resources, which make it impractical for small organizations. Exosphere combines advanced anti-malware capabilities with advanced data protection capabilities, to offer a single easy-to-use, yet comprehensive solution for ensuring your business is secure.

Exosphere

Exosphere is dedicated to protecting your business from multiple cyber threats. Our mission is to provide the optimized endpoint protection solution into the workplace and enhances the business secure and effective. We ultimately value you to offer multiple services and save cost with limited IT staff to enjoy this comprehensive solution.

Exosphere, Inc.
inquiry@exospheresecurity.com
getExosphere.com

"Protect Your Endpoint,
Keep Your Business Safe."

getExosphere.com