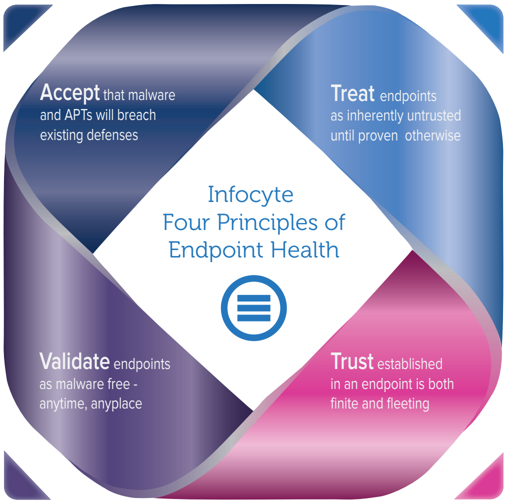
Infocyte®

CONTROLLING DWELL TIME

The importance of defining and managing the breach detection gap


Accept that malware and APTs will breach existing defenses
Treat endpoints as inherently untrusted until proven otherwise
Infocyte Four Principles of Endpoint Health
Validate endpoints as malware free - anytime, anyplace
Trust established in an endpoint is both finite and fleeting

INFOCYTE'S FOUR PRINCIPLES OF ENDPOINT HEALTH

Accept that malware and APTs will breach existing defenses

- Malicious software and advanced persistent threats stay ahead of the defensive curve. It is inevitable that some malware will breach defences.

Treat endpoints as untrusted, until proven otherwise

- Because defences cannot be relied on for total security, endpoints must be viewed as inherently compromised, until their status is established.

Trust established in an endpoint is both finite and fleeting

- Once an endpoint is validated as clean, that status cannot be expected to last.

Validate endpoints as malware free, anytime, anyplace

- The capability to establish the compromise status of endpoints, wherever they may be and at any given point in time must exist.

The Dangers of Dwell Time

Dwell time, also known as the breach detection gap, is the time that exists between the first execution of malware within an enterprise and its discovery. It's an important concept because this gap - between the successful breach of defences and the later detection of malicious activity - poses one of the greatest threats to an organisation's data and systems.

Malware is constantly evolving and recreating itself. New and devastating attacks are regularly in the news, whether the malware being used is a brand new program, a modification of old malware or leaked nation state attack tools made available on the internet.

To make matters worse, primary breaches often facilitate the seeding of secondary malware, RATs, backdoors and other advanced persistent threats. In such cases, by the time the causal program is noticed - usually due to data breaches, customer complaints or notifications from authorities - the malicious actors have been at work for some time and have established other means to return to an enterprise's systems.

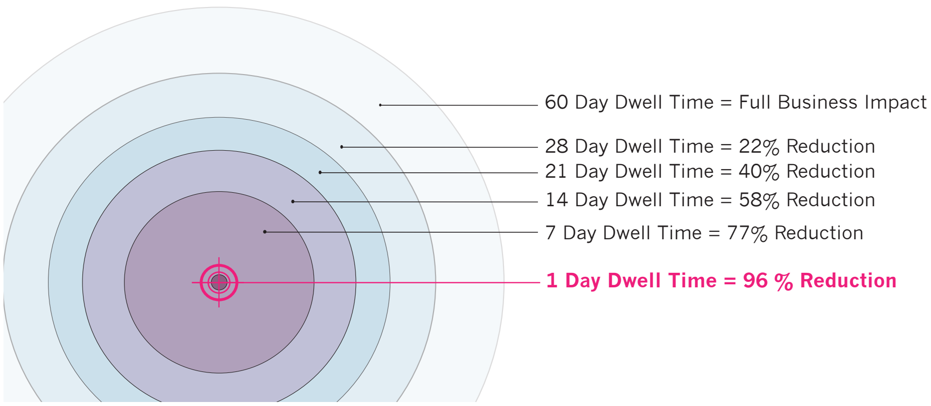
The dangers of dwell time are clear, however the statistics would seem to indicate that organisations do not have the capability to combat these risks. The average dwell time in EMEA is 106 days. Things are even worse in APAC, where malware resides undetected on average for a shocking 172 days before being detected.

Business Impact of Controlling Dwell Time

Organisations require the ability to control and limit dwell time, if they are to begin properly and effectively protecting their data and systems. The negative consequences of allowing dwell time to remain unchecked range from financial losses and damage to reputation, to full system failure.

The combined impact on business has been studied and quantified. A 2016 research report[1] determined that simply limiting dwell time to 30 days results in a reduction of the impact on business by 23%. Further reductions in dwell time lead to a virtual eradication of the business impact, as seen in this diagram.

Controlling Dwell Time Protects Business



[1] Quantifying the Value of Time in Cyber-Threat Detection and Response, Aberdeen Group, February 2016

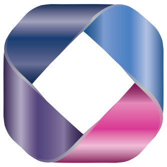
Best Practices to Reduce Dwell Time

Given the constant evolution of threats, and the inability of defences to keep up, it is virtually impossible to erase dwell time. Malware will continue to breach defences. What is required is the capability to control dwell time and dictate how long malware and APTs are allowed to persist undetected.

Infocyte has developed a solution to drastically slash dwell time. We presume endpoints are already compromised, and have developed a solution that not only hunts malware that has breached defences, but also equips users with the capability to verify that endpoints are 'clean'. This endpoint validation can be scheduled regularly, or run on demand.

Our approach is premised on four basic principles, that can help guide enterprises in taking a proactive stance to combat malware and APTs.

1. Accept that malware and APTs will breach existing defences.
2. Treat endpoints as untrusted until proven otherwise.
3. Trust established in an endpoint is both finite and fleeting.
4. Validate endpoints as malware free, anytime, anyplace.



When these principles are put into practice, using Infocyte HUNT, enterprises acquire the capability to define and manage their dwell time. Risk tolerances will vary by industry, but Infocyte's platform is scalable and users dictate scan frequencies to suit their requirements. Banks, for example, are able to scan enterprise workstations and ATMs daily if desired.

Use Cases

Aside from the obvious business advantage of controlling dwell time, there are additional benefits to adopting Infocyte HUNT.

REDUCING THE TIME AND COST OF INCIDENT RESPONSE

Infocyte HUNT equips IT teams with preliminary analysis of identified threats, allowing IR resources to confidently focus their time and energy on clear and present dangers.

Regular scans mean that the data required by response teams is contained to a smaller window of time, resulting in faster incident response because the volume of data to review is manageable.

Faster IR is more cost effective, freeing up budget for more frequent engagements.

BOARD AND EXECUTIVE ASSURANCE

The attention of senior management and board members has now expanded to include data security and protocols to protect enterprise data.

Adopting Infocyte HUNT allows IT teams to validate endpoints regularly and obtain easy to read reports that conclusively determine the compromise status of endpoints.

Provided with reporting proof, board members and executives can rest assured that endpoints are diligently monitored.

RISK MANAGEMENT AND MITIGATION OF LIABILITY

Current regulatory requirements and data breach disclosure laws have created a framework for legal ramifications for enterprises that ignore dwell time.

The first civil action claiming that enterprises should be held liable for losses due to allowing lengthy dwell time was filed in 2016[2].

Deploying Infocyte HUNT enables organisations to define and manage their dwell time, demonstrating organizational due diligence and mitigating legal risks.

[2] Case 1:16-cv-02247, Selco Community Credit Union v. Noodles & Company, Class Action, Sept 2016.

Infocyte®

CORPORATE HEADQUARTERS
110 E. Houston St. Floor 6
San Antonio, TX 78205
+ 1.844.INFOCYTE (844.463.6298)
sales@infocyte.com

www.infocyte.com
@InfocyteInc