VIAVI Solutions

White Paper

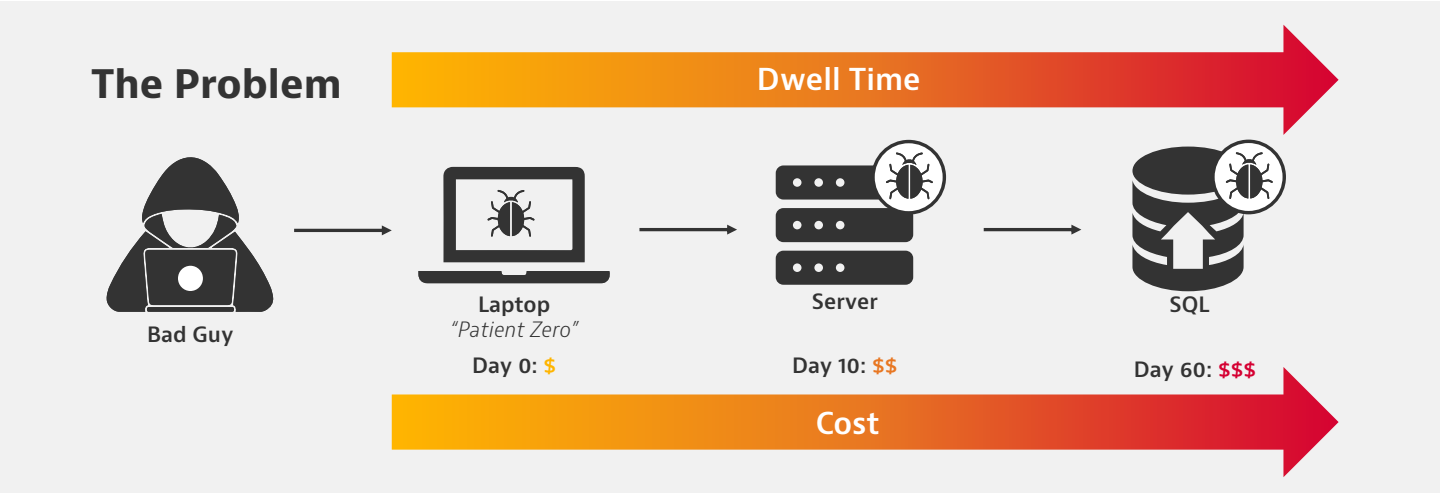
How to Protect Your Business by Limiting Attack Dwell Time

Relentless cyberattack is a fact of life for businesses of all kinds, made worse by the recent surge in remote work, which has put endpoint security under greater pressure than ever.

As bad actors gain access to valuable data, companies are paying the price in remediation costs, legal fees, customer disaffection and loss of corporate reputation.

Every breach, on average, costs $3.86 million.[1] Some attacks, however, have a catastrophic impact on corporate finances, with total costs spiraling into hundreds of millions of dollars. The cause of many disastrous breaches is extended dwell time, meaning the ability for attackers to stay active and undetected within a targeted organization for sometimes months, enabling them to maximize direct and collateral damage to the business. For example, by implanting malware in a routine software update, the recent Sunburst attack exploited dwell time of several weeks to explore compromised systems for information of value before reporting back to the perpetrators and providing them with command and control over the victims' systems.[2]

Given the persistence of cybercriminals, malicious actors and rogue nation states, there is little chance of avoiding attack. Rather than attempting to prevent incidents altogether, a more realistic strategy is to assume that successful attacks against your IT resources can and will occur—and even that your organization has already been breached. Following this strategy means denying trust to any and all users and entities active in the network. A key goal of such an approach is reducing the dwell time of attacks that successfully penetrate an organization, ensuring stolen data, remediation costs and reputational damage can be kept to a minimum.



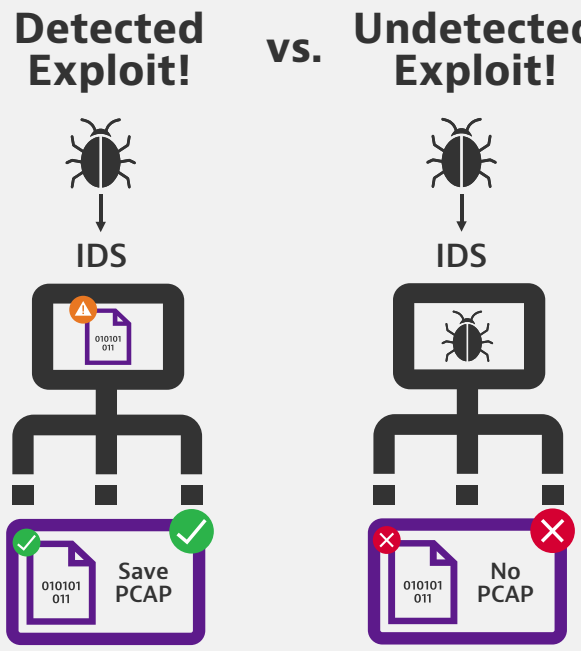
1 "Cost of a Data Breach Report 2020," IBM and Ponemon Institute

2 "Sunburst and the Importance of Evidence-Based Risk Management," VIAVI Perspectives blog, Jan. 5, 2021

TechTarget | Custom Media

Retaining packets, reducing dwell time

Although reducing the dwell time of a threat is essential, the recurrence of catastrophic breaches such as Sunburst is a good indication that doing so is no easy task. To discover attacks as quickly as possible, it is necessary to thoroughly investigate all suspicious incidents by studying data packets, traffic patterns and the behavior of users and devices. Although the ability to observe packets in transit is valuable, the ability to retain packets for further analysis is indispensable for comprehensive forensic investigations, which greatly increase an organization's ability to discover threats and significantly reduce dwell time.



Without packet capture, if malware gets past the Intrusion Detection System, there is a window of time where it leaves no trace.

The malware can probe internally and leave backdoors with no historical record of it.

With regard to zero-day attacks, for example, retaining forensic data for extended periods allows investigators to return to day zero and observe exactly how the compromise occurred. After a zero-day event has been disclosed to the public and a patch has been created, an organization may apply the patch, but the attack might already have penetrated the organization and could still do damage. Only by going back to the time frame of the incident and scouring packets and traffic data can cybersecurity personnel determine whether an organization has been penetrated. This is true not just for zero-day attacks, but for any attack or data exfiltration that avoids initial detection.

The ability to go back in time to observe employee behavior is important as well. An employee who is unaware that their system has been compromised can be a particularly damaging attack vector, as the employee will behave normally, accessing data and applications, all the while unconsciously harboring and transmitting malware.

Similarly, should a worker engage in data theft, it might not be possible to observe the employee's actions while they are in progress. However, correlating the employee's behavior with packet and traffic information over a given time period is very likely to yield information that demonstrates culpability.

In addition, the ability to retain data for further study is a critical tool for investigations related to regulatory compliance. The ability to observe and verify what happened during an incident is vital to a successful defense in a compliance inquiry. For example, the review of historical data can show that personally identifiable information (PII) did not exfiltrate during an incident, demonstrating that compliance with regulations such as HIPAA, GDPR or CCPA was maintained.

Despite these significant benefits, many organizations fail to capture and retain wire data. Why? As data transmission speeds increase, it becomes more difficult and costly to capture and retain all packets or flows for in-depth examination. In addition, data packet analysis packages can be difficult to use. Consequently, some IT leaders simply decide that it is worth saving the cost of technology that enables wire data capture and long-term retention even if it means increasing the risk of suffering a zero-day attack with potentially catastrophic consequences. It's a dubious tradeoff.

The VIAVI Observer platform

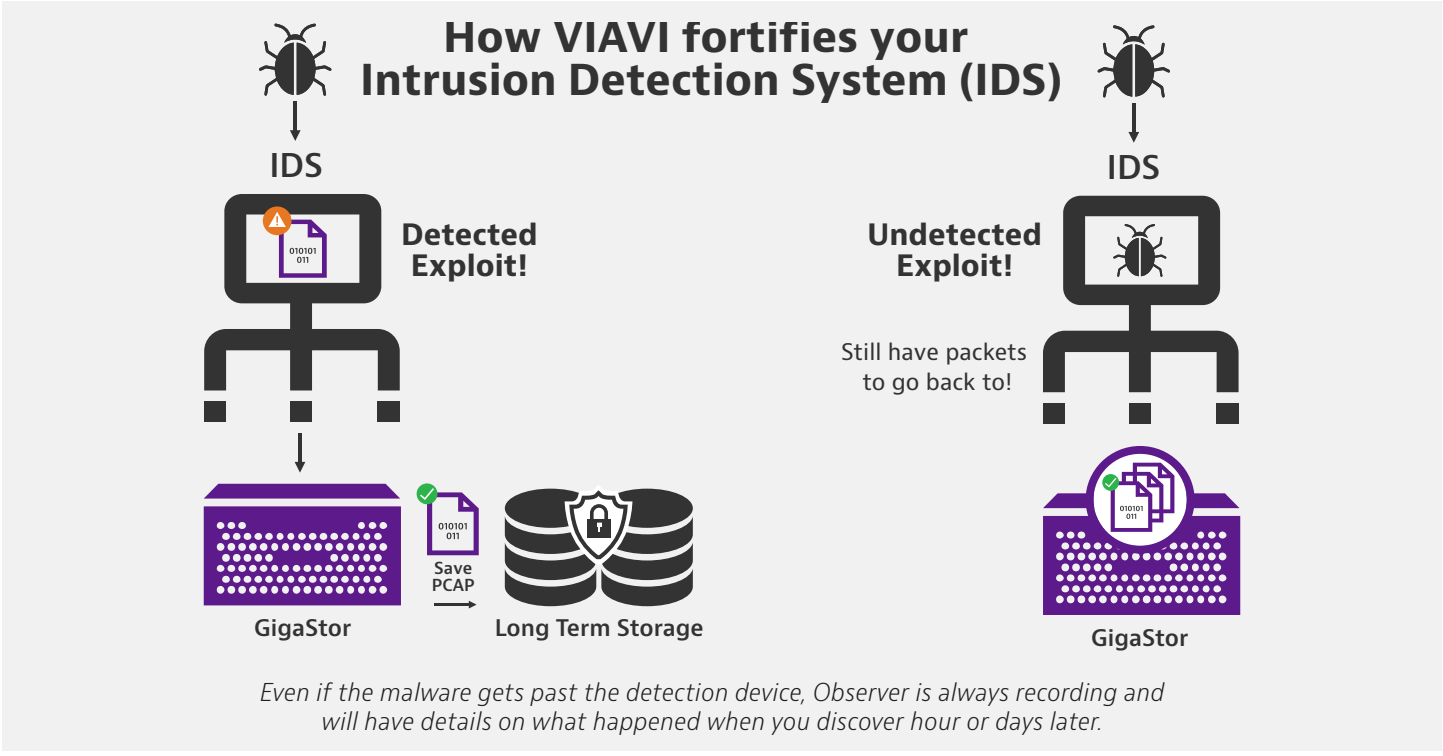
The VIAVI Observer platform includes the VIAVI Observer GigaStor appliance, which performs enriched flow packet capture and analysis. The ability to digest and correlate telemetry information from different network infrastructure devices enables Observer to see which devices are connected and who is communicating in order to identify suspicious events. Observer discovers whether data was exfiltrated and, if so, what the data was. Observer's machine learning capabilities ascertain the severity of an event's impact on the end-user experience.

Integrated threat analysis

Combining the packet capture capabilities of Observer with other cybersecurity capabilities in integrated threat analysis provides numerous benefits. For example:

- **Whitelisting:** Observer's host and service profiling reduces dwell time by proactively identifying abnormal device behavior. Case in point: when a printer is not acting like a printer but handling unusual traffic that might indicate a breach.
- **Fast remediation:** IP Viewer accelerates response and remediation by obtaining answers to security questions in seconds, as opposed to hours or days. These questions include:
  - What was the host or device communicating with earlier?
  - Where is the rogue host or device now?
  - Who was using the host/device?
- **Back-in-time analysis:** Because VIAVI Observer is always recording data traffic, it preserves details of what happened when a breach is discovered hours or days later. For example:
  - Even if a hacker gets past an intrusion detection system, Observer's packet capture will reveal all of the hacker's actions.
  - Such wire data analysis capabilities complement existing security solutions, exponentially increasing their effectiveness. For example, applying an IP blacklist to information retained by Observer can pinpoint whether malicious traffic has entered the network.

Because it is easy to deploy, the Observer platform overcomes a significant obstacle: usability, which has held back many organizations from benefiting from such a solution. ObserverONE is a low-risk, easy-to-deploy performance and threat analysis system. Users can start with a single-box implementation and expand it as network growth demands.



Even if the malware gets past the detection device, Observer is always recording and will have details on what happened when you discover hour or days later.

Conclusion

Business and technology leaders understand all too well that they live in a dangerous world. Cybersecurity threats can be expected to continue unabated while increasing in sophistication. The stakes of defending the organization from financial loss, customer dissatisfaction and reputational damage have never been higher.

The most effective strategy for protecting corporate data and PII is to assume that some attacks have already succeeded and that malware has been implanted in the organization. Discovering attacks, even zero-day attacks, after the fact requires the ability to capture packets and retain them for forensic analysis.

By performing packet capture and retention, the VIAVI Observer platform enables in-depth examination of events well after they have taken place. Through its easy-to-use interface, a network or security operations team member can simply enter a username to immediately find all devices, interfaces and applications associated with it, revealing what is connected and who is communicating across the network.

Observer interoperates with a broad array of security solutions and tools as part of an integrated threat analysis strategy. Starting with ObserverONE, organizations can build their defense incrementally and economically. Most important, Observer reduces the dwell time of active threats. By catching the bad guys sooner, Observer enables an organization to outperform its peers in protecting critical data and PII, delivering a significant competitive edge.

To learn more about how Observer can bolster the cybersecurity posture of your organization, visit **viavisolutions.com/observerdemo**.

Starting with ObserverONE, organizations can build their defense incrementally and economically.

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To learn more about VIAVI Observer, visit viavisolutions.com/observerdemo

viavisolutions.com