Board Ready Endpoint Resilience in 5 Steps

Malwarebytes

Introduction

At the heart of every organization are its employees, the engine that drives growth, fueled by the data they create and store on their laptops, tablets, and mobile phones, as well as access through data center and cloud servers.

It should come as no surprise to CISOs that **60 percent of corporate data is stored on employee endpoints.**[1] And cybercriminals are progressively targeting the valuable data contained on these enterprise endpoints, recognizing the higher return on investment compared to consumer prey. In fact, businesses saw **a 235 percent increase in cyberattacks.** What's even more concerning is that there was over a six-fold increase in information-stealing Trojan malware such as Emotet and TrickBot and over a five-fold increase in ransomware such as Troldesh in 2018.[2]

The job of every CISO is to secure the organization and minimize risk to business operations in the event of an attack. One successful endpoint attack can interrupt employee productivity and bring the business to a grinding halt. In an era when CISOs can no longer prepare for *if* there will be a breach but *when* a successful incident will occur, it's more important than ever for organizations to adopt a proactive posture of endpoint resilience.

[1] Helpnetsecurity. Is GDPR-regulated data lurking in unexpected pockets of your organization?. February 2018. [2] Malwarebytes. Cybercrime Tactics and Techniques Research Report. April 2019.

200% increase

in cyberattacks against businesses from 2018 to 2019

Establishing endpoint resilience minimizes the impact of a cyberattack and restores employee endpoints and operational systems to ensure business continuity. **CISOs need to move beyond protection-only measures and adopt endpoint resilience through these five essential steps:**

1. **Prepare**
2. **Protect**
3. **Isolate**
4. **Remediate**
5. **Investigate**

1 Prepare

When it comes to endpoint resilience, the old adage “plan for the worst, hope for the best” holds true. Preparation ensures rigor is applied to your organization’s incident response methodologies. For example, conducting gap analyses ensures that your enterprise can contain the impact of incidents, bringing cloud and on-premise networks, endpoint systems, and applications back to a healthy state as quickly as possible.

Most importantly, when your organization experiences an attack, a prepared, nimble staff can react quickly and effectively.

1 Prepare

KEY CAPABILITIES

CISOs should consider preparation as the starting point of developing a resilience plan—one that evaluates your readiness of people, processes, and technology. Preparation requires that you have identified your most critical assets and that your incident response (IR) team knows **which processes, endpoints, and systems are essential for the company to remain operational when an incident occurs.**

While your IR team is at the heart of preparation, this step should be a company-wide effort. Include key stakeholders across departments in your planning, such as human resources, finance, marketing, customer service, IT, and security operations to establish procedures for communication escalation paths. Organizations are constantly evolving and changing, so it's also important to regularly conduct red team exercises that evaluate and test your company's preparedness.

RECOMMENDATIONS

The required techniques and intelligence for your endpoint security should include:

- Invest in an endpoint security platform that easily integrates with your IT, security operations, vulnerability, and threat management infrastructure
- Create an asset map that identifies the most critical, high priority data stored on endpoints, the network, and in the cloud
- Develop an incident response plan, policy, and procedures that prioritize endpoint remediation based on business criticality
- Collect and disseminate contact information for key personnel and on-call staff
- Run red team incident response exercises, at least annually, that extend to full endpoint remediation

2 Protect

Cybercriminals use multiple vectors to deliver a successful attack. The most effective way to counter the multiplicity of attack methods is through protection diversification. An interlocking web of matching and signature-less technologies work together to not only block known and unknown malware at execution, but also prevent deployment on the endpoint. If we've learned nothing else from the past two decades, we know attackers like to change up their methods.

Endpoint protection that applies multiple techniques to break the attack chain will provide your best defense against the threats of today and tomorrow.

KEY CAPABILITIES

There are many ways employees conduct work on their endpoints. Threat actors try to find a "hook" into each of them, so CISOs need to look holistically at their endpoint protection mechanisms to ensure complete coverage. **Web protection prevents your employees from accessing malicious websites, ad networks, and IPs.** This is especially helpful for safeguarding against malvertising, malspam, phishing, botnets, adware, PUPs, and malware servers.

Your endpoint protection must also include capabilities for application hardening, which applies techniques to prevent your endpoints from being compromised through software vulnerabilities. Once an application is shielded, it cannot be exploited through any of its present or future zero-day vulnerabilities.

Threat intelligence also plays a key role in your endpoint protection. Your protection layers should be powered by threat feeds based on endpoint remediation telemetry, honeypots, and human intel. Threat intelligence with strong representation from active endpoint incident responses generates an informed telemetry of data on the latest malware and other threats.

Most importantly, your endpoint protection must simultaneously use multiple techniques to prevent malware from successfully landing on the endpoint. This should include a mix of static and dynamic approaches, including rule-based detection and behavioral- and AI- or machine learning-based analysis.

2 Protect

RECOMMENDATIONS

The required techniques and intelligence for your endpoint protection should include:

- Web protection that prevents users from accessing malicious sites
- Application hardening to reduce potential for reverse engineering or tampering with apps deployed on the endpoint
- Exploit mitigation that blocks attempts to abuse vulnerabilities and remotely execute code on the endpoint
- Application behavior monitoring and analysis to ensure they aren't abused to infect the endpoint
- Anomaly detection machine learning that identifies viruses and malware based on anomalies from known and good files
- Payload analysis that applies heuristic and behavioral rules to identify entire families of known and relevant malware
- Integration of endpoint threat intelligence telemetry with IT, security operations, vulnerability, and threat management systems to enable rapid response to attacks

3 Isolate

When a successful attack occurs, it happens fast. Automated malware can wreak havoc within seconds of execution, moving laterally from “patient zero” to infect other endpoints within your network segment. Therefore, isolation capabilities are critical for endpoint resilience. While traditional fixed-perimeter security controls such as firewalls and intrusion detection systems can prevent attacks from entering the network, they are rendered useless against an infection’s lateral movement.

Containing an attack at the endpoint stops the bleeding and provides your IR team with the critical breathing room needed to ensure their efforts are applied to the most important areas for effective response.

3 Isolate

KEY CAPABILITIES

Isolation-based capabilities create an air gap between the compromised endpoint and the other systems within your organization. **To achieve endpoint resilience requires the means to contain the infection through network, device, and process isolation.** These containment mechanisms will also impede the malware from phoning home to receive command-and-control communication, which restricts it from doing further damage.

Automation here is essential. A key factor in improving incident response processes is lowering mean time to response (MTTR) or dwell time, and automated isolation methods will significantly aid in this area. In addition, **ransomware infections have increased 195 percent between 2018 and 2019[3], so organizations need to include recovery from ransomware attacks as a requirement of their endpoint isolation.** This capability should include just-in-time endpoint backups that allow you to wind back the clock and negate the impact of a ransomware attack.

[3] Ibid

3 Isolate

RECOMMENDATIONS

The list below provides tools and processes for your endpoint isolation efforts. We suggest you invest in:

- Network isolation that restricts all endpoint-initiated processes from communicating
- Process isolation that prevents new processes from starting up on the endpoint
- Device isolation that stops further interaction to limit damage
- Ransomware rollback, which restores the device to its previous state even after an attack does its damage over a long weekend

4 Remediate

Organizations frequently rely on reimaging to remediate malware-infected endpoints—an expensive approach that is known to cost over $1,000 per endpoint by some accounts. For some IR teams, malware removal tools are used to manually remediate endpoints one-by-one. In the event of a significant attack, time-consuming remediation approaches don't deliver efficient or rapid time to response. In fact, **21 percent of security professionals claim their main barrier to effective incident response is too much time needed to detect and remediate an incident.**[4]

For optimized endpoint resilience, empower your IR team to actively respond by orchestrating across your IT systems' management workflows to remediate endpoints at scale and significantly reduce your organization's MTTR.

[4] SANS Institute. 2018 SANS Incident Response Survey. 2019.

4 Remediate

KEY CAPABILITIES

Technologies that provide thorough and automated remediation will restore your endpoints to their pre-infected, trusted state. Most solutions only remediate active malware components, which falls short of providing complete remediation.

For modern endpoint resilience, your endpoint remediation capabilities should include detection and removal of dynamic and related artifacts. Remediation must apply associated sequencing to ensure malware persistence mechanisms are permanently removed. **Advanced remediation methodologies provide your organization with expedient malware identification and complete removal.**

4 Remediate

RECOMMENDATIONS

Organizations should adopt the following mechanisms and processes to optimize endpoint remediation:

Active response capabilities

- On-demand and scheduled endpoint scanning
- Non-persistent, dissolvable endpoint remediation agents
- Operators and policy with detailed remediation tasks and the ability to automatically restore the endpoint
- Sequencing that identifies and thoroughly removes threat artifacts associated with the primary payload

Enterprise endpoint orchestration capabilities

- Integration with existing security orchestration tools that deliver visibility and agency to coordinate, inform, and execute remediation efforts
- Cloud-based management of endpoints using attack pattern and remediation maps for coordinated red team progress tracking
- Group-based policies and deployment tools to implement endpoint commands and send system updates

5 Investigate

Sophisticated malware dwells long after the initial detection. Dormant code remains hidden on infected devices, patiently biding time for the right moment to strike. Investigations of persistent threats were often considered a luxury only afforded to the largest of enterprises with red teams, complicated-analytics-powered technologies, and highly mature SOC operations. However, economical dark web marketplaces now make it possible for cybercriminals to broadly target any organization. Therefore, companies small and large must have access to tools allowing them to cost effectively conduct investigations that restore the network after an attack and run proactive investigations to maintain a healthy state, rather than waiting for a payload to activate.

Adopting the "assume-the-compromise" posture of conducting investigations will greatly improve your endpoint resilience and overall security hygiene.

5 Investigate

KEY CAPABILITIES

To make investigation part of your endpoint resilience, organizations need the ability to readily cross-reference datasets to gain context and identify relationships with other entities or historical activity. Investigations are crucial to resilience and must support agile data exploration with visual data maps that allow your IR teams to identify impacted endpoints, data, users, as well as threat actor details.

Your endpoint security solution should allow your incident responders to run scheduled scans that proactively hunt for recently reported indicators of compromise (IOCs). On average, cybercriminals spend 191 days inside the network before being discovered[5]. Adopting threat hunting endpoint investigation mechanisms ensures you're discovering these hidden threats.

[5] Ponemon. 2018 Cost of Data Breach Study. July 2018.

5 Investigate

RECOMMENDATIONS

Your endpoint investigation capabilities should include the following tools and processes:

- On-demand and scheduled endpoint scanning for custom IOC threat hunting
- User-initiated remediation scans enabled through integrations with your existing IT systems management tools
- Continuous monitoring for suspicious files and process events, network connections, and registry activity
- Asset management that collects and displays endpoint details (e.g., installed software, updates, and startup programs)
- Visual graphs to investigate processes spawned by a threat and where it moved laterally

Conclusion

There's one thing organizations can count on: cybercriminals will continue to innovate and evolve their techniques. Companies of all sizes need to plan for a successful attack. In today's world of dissolving perimeters, the endpoint is now the new first line of defense against security breaches. For a CISO, that means endpoint resilience is a no longer a luxury, it's a necessary imperative.

Adopting a framework for endpoint resilience that includes preparation, protection, isolation, remediation, and investigation will minimize the impact of a cyberattack and ensure your IR team can act rapidly to restore systems and maintain business continuity.

Malwarebytes: making endpoint resilience a reality

Malwarebytes makes it possible for companies to establish and maintain endpoint resiliency by giving security professionals the tools they need to prepare, protect, isolate, remediate, and investigate attacks.

Our solution is powered by multiple layers of analytics and advanced machine learning to deliver adaptive attack protection that predicts an attacker's next move and applies the right protection techniques at the point of attack. What's more, Malwarebytes provides CISOs with a cost-effective approach to endpoint resilience that is integrated with leading IT and systems management tools, including ServiceNow, Splunk, and Phantom. And granular isolation control options contain infected endpoints by preventing network communications, new processes, and complete access to the endpoint.

Once isolated, security professionals can efficiently remediate with one-click—removing the malware and all attack traces detected through our proprietary Linking Engine technology. Up to 72 hours of ransomware rollback protection restores encrypted, deleted or modified files—returning the endpoint and valuable data to a known, good state without costly reimaging. Lastly, Malwarebytes delivers on the final stage of resilience with simplified tools built for security professionals of all abilities—not just those with PhDs—that can readily be used to conduct proactive and cost-effective investigations.

Take your first step to endpoint resilience

For more information about how Malwarebytes makes endpoints resilient, visit:

malwarebytes.com/business/endpointprotectionandresponse/