WHITE PAPER

Protecting the Cloud in a Hybrid Work World

Securing Critical Assets Requires a New Approach to Endpoint Security

Executive Summary

Remote workers accessing cloud-based services will only become more common in the foreseeable future. Securing these interactions requires a new approach to endpoint security. Rather than passively waiting for a file-matching malware signature to enter the network, the latest endpoint detection and response (EDR) tools help organizations take a more proactive approach to security. Integrating EDR tools into a larger cybersecurity mesh architecture (CSMA) compounds the benefit.

As they evaluate EDR solutions, organizations should insist on several critical capabilities. First, the solution must enable assessment of the attack surface so that gaps can be filled. Next, they must be proactive in malware prevention, taking both signature-based and behavior-based approaches. Then they must be able to detect attacks and defuse them before they cause significant damage. The EDR solution must automate threat response and remediation and enable comprehensive forensics and threat-hunting capabilities to prevent future attacks.

Endpoint Challenges in the Cloud

As the world of work embarks on a work-from-anywhere model for businesses in all industries, it is clear that remote and hybrid work arrangements are here to stay.[1] One study found that 94% of organizations have implemented some sort of hybrid work structure, and 69% say that these new ways of working are impacting everything from office space to IT staffing.[2]

Of course, there are cybersecurity implications to the trend as well. The logistics of enabling work from a variety of locations expands the attack surface, and can even increase the number of endpoints requiring protection from internal and external threats. This is compounded by the increasingly advanced threat landscape that forces organizations to prepare for endpoint attacks from a growing number of vectors.

Remote workers and the cloud

Organizations' swift move to cloud-based services adds another layer of complexity to securing corporate assets accessed by a far-flung workforce. By all accounts, the COVID-19 pandemic accelerated already rapid cloud adoption as organizations scrambled to build or expand work-from-home infrastructure, and customers demanded more digital services.

One recent survey found that nearly two-thirds of IT professionals now expect their organizations to have 60% of their IT services in the cloud within two years.[3] But in many cases, workers at home or in a coffee shop already interact chiefly with Software-as-a-Service (SaaS) applications or services delivered through cloud-based infrastructure, with little need to access the corporate data center at all.

Cloud technology has clearly become key to helping organizations grow and thrive in today's digital environment. It's hard to overstate its importance in enabling companies to support a sudden move to fully remote work at the beginning of the pandemic and survive ongoing supply chain issues, increasing costs, and a rapid evolution in customer preferences and expectations.

Yet the rushed nature of the changes that organizations have made in recent years means that security has not kept up in many cases. Many express concerns around cybersecurity threats like malware, but fewer have moved forward with more robust approaches to endpoint protection, especially when it comes to cloud-based resources. Unfortunately, bad actors only take seconds to carry out advanced attacks against compromised, cloud-connected endpoints.

Cloud-specific challenges

Cybersecurity teams would have plenty of challenges even if cloud-based services did not exist. But cloud platforms are different from on-premises infrastructure in many ways, and securing them requires an understanding of the unique security challenges of the cloud. Some of these challenges include:

- **Inadequate cloud security protocols.** Companies with weak cloud security protections increase their risk of becoming the target of attackers with advanced tools. Not maintaining robust cloud security hygiene practices leaves businesses blind to issues like previous suspicious network activity, a failure to update security patches, and vulnerabilities in cloud endpoints.
- **Slow response.** Bad actors use reconnaissance to look for ways to go after an organization's security weaknesses before the company responds. These attacks cause the most damage because they give the attackers time to work around a company's security defenses. Some attacking organizations only develop and sell intrusions (for example, Cobalt Strike Beacons), so more capable attack groups can focus on causing damage and extracting payment from victims.
- **Cloud misconfigurations.** Improperly secured cloud endpoints allow cyber thieves to hijack data for their purposes. A lack of knowledge of cloud security policies can result in mistakes in implementing cloud infrastructure.

Organizations need to understand the risks, put the right controls in place and apply them to a distributed workforce because the ability of a business to work remotely is paramount.[4]

The importance of robust EDR tools

The increasing complexity of threat actors and the specific challenges posed by remote workers using a hybrid-cloud architecture highlight the need for a new approach to endpoint security. Moving beyond signature-based antivirus and intrusion protection, EDR solutions seek to move organizations from reactive threat response to proactive risk mitigation.

Yet some organizations that deployed EDR some time ago are seeing management issues today. One reason for this is that first-generation EDR tools require significant manual intervention, slowing response times when security incidents occur. Delays in proactive threat response bring the risk of production shutdowns and system disruptions for end users. Newer EDR solutions automate incident response (IR), defusing threats quickly enough to minimize damage at the point of entry and prevent their lateral move across cloud clusters and connected networks.

What to Look for in an EDR Solution

Effective EDR solutions address deficiencies in endpoint security by providing future-facing, real-time threat protection before and after an endpoint attack. This allows organizations to reduce the attack surface proactively. A next-generation endpoint protection solution also provides organizations with broad detection, prevention, and response capabilities in a lightweight framework that companies can deploy even on devices without a lot of system resources.

Organizations should ensure that their EDR solution helps them accomplish the following:

Discover and reduce the attack surface

A superior EDR solution provides advanced, automated attack-surface policy controls. This includes the ability to conduct vulnerability assessments and create policies for automation vulnerability management. Organizations can also use the technology to look for gaps and weaknesses in their protection. An EDR tool should be able to:

- Locate and control unprotected and unmanaged devices
- Provide complete insight into vulnerabilities with ratings and reputation
- Mitigate attacks leveraging vulnerabilities with virtual patching

Using the proactive risk mitigation functions available within an EDR solution helps reduce the number of unprotected endpoints within an organization, effectively decreasing the attack surface open to attackers.

Prevent malware

New advanced tools have made it easier for cybercriminals to launch malware attacks against vulnerable cloud endpoints. One prominent example: Ransomware-as-a-Service (RaaS) providers have enabled even non-experts to carry out devastating ransomware attacks against organizations in all industries and all sizes. This is one factor that has led to sharp escalation of such attacks in recent years.

Rather than relying solely on signatures of existing malware, it is now essential that organizations use behavior-based anti-malware technology, sometimes called next-generation antivirus (NGAV). This helps stop new malware before it spreads laterally within on-premises and cloud-based networks.

Organizations also need to prevent malware attacks on endpoints not connected to the internet, including many operational technology (OT) systems. Many of these run on older operating systems with critical vulnerabilities that cannot be updated. For such systems, organizations should look for endpoint security solutions that can run in simulation mode before putting them into production.

EDR tools should have these critical malware prevention capabilities:

- Behavior- and kernel-based NGAV that can arrest attacks
- Integrations with real-time threat intelligence feeds that receive continuous updates
- Application control to help lock down sensitive systems
- Remediation tools
- Automatic IR with customizable options to create granular policies
- Threat-hunting capabilities

Detect and defuse attacks

Even with the best malware defenses, attacks inevitably make their way to cloud systems. When this happens, an EDR solution should be able to disable attacks in real time. Stopping attacks as they execute before they can cause damage is key for preventing breaches and reducing the risk of data loss and the need for repair.

Once the artificial intelligence (AI) within the EDR solution detects any suspicious activity, like unusual flows or process behavior, it should immediately defuse the threat by blocking any attempts to send outbound communications. In addition, the threat should not have the opportunity to access other cloud structures, connected devices, or networks. Some examples of what EDR should prevent malicious software from doing are:

- Extracting data
- Enacting command-and-control (C2) communications
- Tampering with files and registries
- Encrypting files
- Opening backdoors

Organizations should look for these related capabilities to further ensure they have the ability to stop the effects of a potential breach:

- Detect attacks, including memory-based and “living-off-the-land” attacks
- The ability to analyze an entire log history
- Ongoing validation of threat classifications

Respond and remediate

The main way organizations smoothly respond to and remediate policy violations is by orchestrating IR operations. This should be done with customizable playbooks designed for each group based on user, device type (such as a server), and cloud. When an attack has executed, these organizations enact manual or automatic rollbacks of any system changes on single or multiple devices within an environment, including the cloud. This makes it possible for security personnel to:

- Automate the classification of security incidents
- Create standardized IR procedures enacted through playbook automation

Organizations can optimize security resources by automating things like:

- File removals
- Termination of malicious processes
- Persistent change reversals
- Application and device isolation
- Opening of tickets

As the threat landscape continues to become more sophisticated, a real-time approach is critical to address the advanced threats targeting endpoints and address the cyber skills shortage.[5]

Investigate and hunt

Another feature to look for in an EDR tool is the automatic use of information gathered on malware actions before and after infection to conduct forensics on affected endpoints. Security analysts should have access to a guided interface that contains detailed suggestions on best security practices and the logical next steps to proceed when evaluating a possible threat.

The best solutions offer visibility into the entire attack chain with the ability to preserve memory snapshots of in-memory attacks. The interface should offer clear explanations about the reasons behind flagging an event as suspicious while listing the corresponding tactic, technique, or procedure (TTP) from the MITRE ATT&CK Matrix.

How to Architect an EDR Solution

When selecting an EDR solution, organizations should consider the tool's capabilities and how it will work in their infrastructure and with their cybersecurity workflows.

Integrations with the security infrastructure

It is critical that EDR tools be a part of what Gartner calls a Cybersecurity Mesh Architecture (CSMA), integrating with other parts of the security infrastructure. Taking a broad, integrated, automated approach to the security architecture unlocks many possibilities that improve the EDR's effectiveness, such as:

- Isolating devices from the network into a remediation virtual local-area network (VLAN) via the network access control (NAC) tool
- Preventing follow-on attacks by blocking a malicious IP address using a next-generation firewall (NGFW)
- Better understanding of the forensics of an attack through integrations with security information and event management (SIEM) and security orchestration, automation and response (SOAR) tools

While a number of vendors integrate their own security offerings, it is also instructive to see what third-party solutions they support with predefined actions that can be triggered through automation. If a vendor does not support a component of the security architecture, an organization should look into whether an application programming interface (API) is available to create an in-house integration.

Managed options

For organizations that do not have experience with an EDR tool or lack a dedicated security operations center (SOC) team, the change from older anti-malware technologies to a behavior-based endpoint solution can be a significant shift. Such companies often look to a vendor that provides a managed option to assist in managing their EDR solutions' alerts, investigations, exception building, reporting, and more.

For organizations that go the managed route, here are some criteria to look for:

- All staff are full-time members of the vendor's staff and not contractors
- The vendor's managed EDR staff is located in the same region(s) as the local team(s)
- The staff of the managed offering is also trained in other security technologies that are integrated with the EDR solution, such as firewalls, ticketing systems, NAC, or SIEM

A cybersecurity mesh architecture (CSMA) helps provide a common, integrated security structure and posture to secure all assets, whether they're on-premises, in data centers, or in the cloud.[6]

Conclusion

Remote and hybrid work arrangements are here to stay, as are cloud-based services. This is a potentially explosive combination that requires a new approach to endpoint security. An EDR solution should defend both in-house and cloud-based services from cyberattacks originating both inside and outside the organization. It should have critical capabilities that include:

- Behavior-based anti-malware detection
- Rogue device discovery
- Threat hunting
- Virtual patching
- Forensic investigation
- Real-time attack blocking
- Automated IR

The best EDR tools rely on an integrated CSMA architecture that seamlessly meshes with other security components, enabling the entire security architecture to work together to prevent attacks, respond quickly to them when they happen, and conduct thorough forensics after the fact to prevent similar attacks from happening again.

Learn more about FortiEDR on Google Cloud Marketplace

Google Cloud

[1] Liam Tung, "Hybrid Work Is here to Stay, So Companies Are Spending More on Security," ZDNet, June 28, 2022.

[2] Ibid.

[3] Joe McKendrick, "Rush to Cloud Computing Is Outpacing Organizations' Ability to Adapt," ZDNet, March 5, 2022.

[4] "The Security Challenges of Hybrid Working," Verizon, accessed August 16, 2022

[5] _ David Finger, "Endpoint Detection and Response is a Key Weapon in the Battle Against Ransomware," CSO, May 24, 2021.

[6] Gartner®, "Top Strategic Technology Trends for 2022: Cybersecurity Mesh," Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Buddy, Patrick Havesi, 18 October 2021.

FORTINET®

www.fortinet.com

September 1, 2022
1687342-0-0-EN