SIX ESSENTIALS TO PROTECT ENDPOINTS FROM DATA BREACHES

magna5

www.magna5global.com ☎ 844.624.6255

Cybercriminals are launching waves of relentless attacks against remote workers, sparking an urgent need for advanced, real-time threat prevention, detection and response that protects all perimeters – networks, virtual clouds, remote offices and mobile operations.

The way today's workforce performs work has changed. Employees are more commonly working remotely using endpoints that are no longer living in the compounds of a "secure office." This results in broader attack surfaces for cyber criminals to find entry footholds into your network without you even knowing it.

No question, hackers are zeroing in on endpoint vulnerabilities created as millions of Americans work from home due to the pandemic. An estimated 70% of breaches start on endpoint devices. When working remotely, there's a hidden security danger. All those endpoints and devices connected outside of the office firewall are prime entry points for cybercriminals to target your organization. Without proper protection, it's open season for a tsunami of malicious ransomware attacks through those unsecured endpoints.

Why Are Endpoints Commonly Attacked?

Endpoints are the heart of a cyberattack. Threat actors use them as a gateway into your network and as the first building block of an attack. If left unsecure, endpoints provide easy access to critical information that can help the bad guys spread an attack and infiltrate other critical systems. Once an endpoint is breached, threat actors can gain access to admin credentials, process actions, file access information, network events, endpoint configuration changes, passwords and more. Endpoints are also usually linked to each other, allowing threat actors to move laterally across other machines.

On top of endpoints being data and information-rich, endpoint protection relies on employees to make smart, security-conscious decisions. According to the 2021 Data Breach Investigations Report by Verizon, 85 percent of breaches involved human error. Employees are one of the largest attack vectors. Through malicious intent or negligence, your employees' behaviors determine the success or failure of your endpoint security.

Hackers and threat actors are relentlessly seeking new ways to infiltrate your endpoints and sophisticating their techniques to bypass preventative solutions you have in place. They have even started to work together. In 2019, 55 percent of breaches were committed by organized criminal groups. These bad guys are building relationships between different groups to increase the odds of breaking and entering into your business' sacred information.

Now that we know why threat actors target endpoints, let's look at some of the most common types of endpoint attacks.

Types of Endpoint Attacks

Today's threat actors are leveraging ransomware and other malware through phishing lures, malware distribution and domain registration tied to COVID-19. Common themes include scamming, brand impersonation, blackmail and business email compromise.

They use a variety of methods to gain access to business systems to obtain money, personal identifiable information (PII) and username and passwords. Many threat actors use fear tactics and big world events to scare their victims into making poor security choices. Here are the most common types of endpoint attacks:

1. Phishing

A phishing attack is a type of social engineering attack used to steal user data like passwords, credit card information and PII. A threat actor will disguise as a trusted entity to trick a victim into opening an email, text message or instant message that contains a malicious attachment or link. Once the link or attached is clicked on, malware is installed that gives the threat actor access to your system and data. Phishing is often used to gain a foothold in networks as part of a larger attack.

According to the IBM Cost of a Data Breach Report, 90 percent of cyber-attacks begin with a phishing attack. 2020 and 2021 were full of coronavirus-themed phishing attacks where threat actors were imitating the CDC or the IRS to trick fearful victims into giving sensitive information up. In November 2020, an SMS-based phishing message was being sent to US residents that impersonated the IRS stating, "Further action is required to accept this payment into your account. Continue here to accept this payment ..." A link directed users to a phishing site imitating the IRS.gov Get My Payment website where victims were asked to share their personal and bank information. [Security Magazine]

2. Ransomware

Ransomware is a form of malware that encrypts a victim's files and demands a ransom to restore access to the data. One of the most common delivery systems of ransomware is a phishing attack. Malware will live deep in the code of an attachment on an email or a link that is disguised to be trustworthy. In 2021, a ransomware attack are taking place every 11 seconds.

In May 2021, threat actors infiltrated the Colonial Pipeline causing mass gas outages for nearly half of the east coast. It is believed that the threat actor gained access by a phishing attempt tricking an employee into downloading malware. It is unknown how long the threat actors were inside of Colonial's network before launching the ransomware attack. When unsure how bad the breach was or how long it would take to get the pipeline back up, Colonial decided to pay almost $5M in ransom to restore information.

3. Zero-Day Exploits

A zero-day exploit is an unknown exploit in the wild that exposes a vulnerability in software or hardware that threat actors can act on or release malware before there is a known fix or patch. Some of the biggest data breaches have been from zero-day exploits such as Petya, NotPetya and the 2021 SolarWinds breach.

In early March 2021, cybersecurity experts uncovered a Microsoft Exchange Server attack that exploited vulnerabilities in Microsoft's on-premises email servers. The attack has been attributed to a Chinese cyber espionage group that aims to steal email contents of user mailboxes from victim organizations. [ZDNet]

Fight Back with Threat Detection and Response

Unfortunately, you can't click your heels three times and magically keep threat actors at bay. In order to have a reliable security posture, you need a multi-level security plan that safeguards your critical infrastructure and data. A combination of intelligent threat prevention and detection tools along with human threat hunters with contextual awareness and response capabilities can help stop attacks before they do serious damage. Let's take a look at how to fight back with six important security measures.

Real-time security risk visibility and proactive alerts

Combining attack prevention (like antivirus, firewalls and DNS filtering) with proactive threat monitoring and detection tools will give you full visibility into what vulnerabilities and active threats are on your endpoints. AI self-learning tools can stop highly sophisticated malware, hacking tools, ransomware, memory exploits, script misuse and other fileless attacks. 24/7/365 proactive monitoring combined with human intelligence ensures you are aware of when an attack is taking place and can stop it before real damage happens.

Granular endpoint management control

Policy-based configurations can kill a process, quarantine or delete malicious binaries before they do any damage on your endpoints. Policy-driven protection allows or blocks USB devices and endpoint traffic to determine the appropriate response.

Visualize attacks with real-time forensics

It is important to see forensic information and storyline visualizations that map out the attack's point of origin and progression across endpoints in real-time. Detailed forensics show the extent of the damage, how the attack happened and how you can efficiently respond to stop the attack. Cross-platform visibility into all endpoints, encrypted traffic and all applications and processes can make sure you are getting all the information needed to stop infiltration.

Eliminate vulnerabilities on your network

Good cyber hygiene starts by ensuring all devices and applications are consistently patched and upgraded. Deep visibility into every device and application running both on-premises and in the cloud allows the entire patching and endpoint configuration process to proactively minimize the vectors that attackers can exploit.

Hunt down the hackers

It's one thing to keep cybercriminals out. But what if they have already compromised your network? Actively hunting for threat actors with sophisticated algorithms seeks out potential footholds and hard-to-detect persistent threat methods.

Close the vulnerability gap between detection and response

Stopping a malicious attack as soon as possible is imperative to minimize the amount of damage already done or data that could be compromised. Many organizations don't have the manpower or resources needed to manage endpoint security. Partnering with a team of security experts who can manage the entire incident response process can relieve IT teams of error-prone manual mitigation procedures.

Closing the Security Gap With Magna5

Magna5's Endpoint Security unifies prevention, detection and response in a single solution backed by a 24/7/365 Operations Center. It provides prevention and detection of attacks across all endpoints regardless of your workforce location, in the office or remote. Magna5 offers patch management, attack detection and active threat hunting with behavioral monitoring, remediation and complete visibility into the endpoint environment with real-time data and incident response. With attackers relentless targeting remote workers, our solution minimizes the risk of threats, like ransomware, so your organization can remain secure without interruption.

Need a multi-layer defense for your endpoint devices? Let us help. Schedule a consultation with our experts.

About Magna5

Magna5 is a nationwide provider of network services, unified communications, infrastructure technology and managed services. By bringing together enterprise-class platforms from leading providers and a 24/7/365 Operations Center, Magna5 has the unique ability to leverage leading software, carrier diversity and customize solutions that drive value to customers and vendors alike.

In working with private and public businesses of all sizes, from government agencies to manufacturing organizations, small businesses and large-scale operations, we believe that focusing on the needs of our clients through a boutique approach to customer service is key. With more than two decades of experience in the managed services and telecommunications industry, we've acquired the experience to understand the needs of your organization, the changing landscape of providers and diverse technologies to deliver targeted, strategic solutions that make a difference.

Whether you need managed services, security services, voice services or are looking to move to cloud-based infrastructures, Magna5 helps your business make smart connections.

magna5

CONTACT US

Corporate Office
3001 Dallas Parkway, Suite 610
Frisco, Texas 75034
844.624.6255
www.magna5global.com