CYBERSECURITY'S MAGINOT LINE:

A Real-World Assessment of the Defense-in-Depth Model

A Report by FireEye and Mandiant, A FireEye Company

CONTENTS

Cover: A simplified diagram of turrets deployed as part of France's Maginot Line in the run-up to World War II.

The upshot:

It doesn't matter what types of firewall, intrusion prevention system (IPS), Web gateway, sandbox and endpoint systems make up organizations' Maginot Line; attackers are circumventing them all.

As this report explains, to protect themselves effectively, organizations need to evolve their security architecture so they do not rely on malware signatures alone. Security teams must be able to see the alerts that matter.

And they must complement those with rapid endpoint response expertise to confirm and contain attacks as soon as they appear.

Executive summary

Today, most people know the Maginot Line as one of history's biggest boondoggles. Constructed at a massive cost to the French government in the run-up to World War II, the 940-mile line proved futile in the face of a new style of warfare.

The Maginot Line didn't fail, exactly. In fact, it held up superbly against several direct assaults. But Germany, employing new weapons and a lightning-fast blitzkrieg attack style, simply sidestepped the line and invaded through Belgium.

The IT security industry faces a similar predicament. Organizations spend more than $67 billion on IT security.[1] Yet attackers routinely breach those defenses with clever, fast-moving attacks that bypass traditional tools. Like the Maginot Line, the prevailing defense-in-depth security model was conceived to defend against yesterday's threats. As applied today, it leaves organizations all but defenseless against determined attackers.

Just how (in)effective are today's defense-in-depth deployments? Unfortunately, industry testing bodies offer little help for organizations looking to assess their defenses. Controlled laboratory settings rely on samples of known threats and assumptions about cyber attacks, which may be outdated or incomplete. They cannot replicate the unpredictable, constantly evolving nature of real-world attacks.

The only true test of a product is in a real-world setting. That is precisely what this report provides. In this report, we present a first-of-its-kind analysis of real-world data from more than 1,216 organizations in 63 countries across more than 20 industries. It reveals a defense-in-depth security architecture that is deeply flawed.

The data comes from organizations testing FireEye network and email appliances but not yet fully protected by the FireEye platform. These tests provide a unique vantage point to observe other security layers in action because FireEye network appliances sit behind all conventional security defenses.[2] Therefore, by definition, any threats observed by FireEye in these tests have passed through all of an organization's other security layers.

Key findings include:

97%

Nearly all (97 percent) organizations had been breached, meaning at least one attacker had bypassed all layers of their defense-in depth architecture.

1/4

More than a fourth of all organizations experienced events known to be consistent with tools and tactics used by advanced persistent threat (APT) actors.

3/4

Three-fourths of organizations had active command-and-control communications, indicating that attackers had control of the breached systems and were possibly already receiving data from them.

1.6

Even after an organization was breached, attackers attempted to compromise the typical organization more than once per week on average.

---

[1] "Gartner Says Worldwide Security Market to Grow 8.7 Percent in 2013," Gartner press release, June 11 2013.

[2] FireEye appliances powered by the patented Multi-Vector Virtual Execution (MVX) engine, monitor Web and email traffic that has passed through firewalls, intrusion detection and prevention systems (IDS/IPS), and Web proxies. Rather than relying on binary signatures, the MVX engine analyzes suspicious files and objects executed within a virtual machine environment. So it detects malicious activity that other defense-in-depth layers miss. FireEye appliances also identify command-and-control traffic from malware not stopped by endpoint tools.

MAGINOT AS
A METAPHOR

FRENCH STATESMAN AND WORLD WAR I LEADER GEORGES
Clemenceau is often credited with the old adage that generals are always preparing for the last war rather than the next one.[3] He never knew how prescient those words would prove.
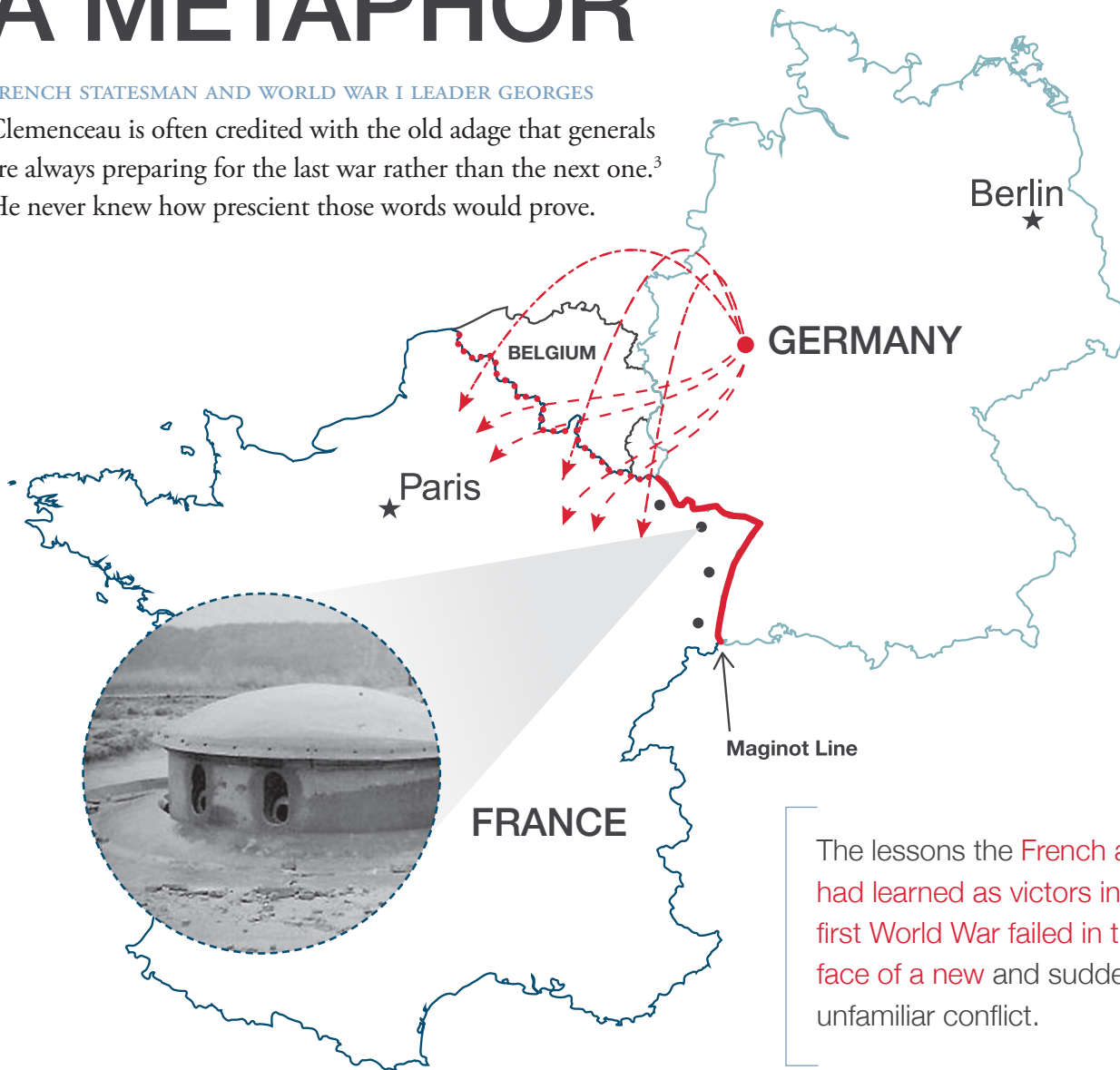
Berlin

GERMANY

BELGIUM

Paris

FRANCE

Maginot Line

The lessons the French army had learned as victors in the first World War failed in the face of a new and suddenly unfamiliar conflict.

Figure 1: A map showing Germany's invasion of France in May 1940. The German army sidestepped with Maginot Line with blitzkrieg-style attacks through Belgium. (Inset) One of the turrets used in the Maginot line. The turrets were embedded deep underground, leaving only the barrels showing above ground.

[3] Valentine Williams. "World of Action." 1938.

A History of the Maginot Line

Just a few years after Clemenceau's death in 1929, France began building the famed Maginot Line, a 940-mile string of deep-earth bunker fortresses, anti-tank obstacles, and barbed-wire entanglements along the Franco-German border.[4] Named after France's then-Minister of War, André Maginot, the line was designed to hold off an increasingly hostile Germany, which bristled under the yoke of WWI reparations.

Hailed as the "world's greatest defense system" in a 1931 magazine article detailing its construction,[5] the line was a technological marvel (see sidebar, this page).

A new age of war

But it was all for naught. By the time Germany invaded in May 1940, warfare had evolved from WWI trench-style combat to fast-moving blitzkrieg operations. Hitler's army sidestepped the Maginot Line with a lightning-fast push through Belgium that caught French and allied forces off guard.

The French military — which had diverted much of its pre-war spending toward the Maginot Line rather than modern weapons — could not reinforce the Belgian front quickly enough. Crushed on the battlefield, France surrendered less than six weeks later. The lessons the French army had learned as victors in the first World War failed in the face of a new and suddenly unfamiliar conflict.

In its time, the Maginot Line was an impressive military feat and one of the most advanced defensive structures the world had ever seen.

The 940-mile string of deep-earth bunker fortresses, anti-tank obstacles, and barbed-wire entanglements lined the Franco-German border, with similar defenses running along the Italian border.

Its largest bunkers featured cannons, antitank mortars, and retractable turrets.[6] Some bunkers reached more than 30 meters deep, providing ample space for as many as 1,000 troops along with food, water, and other supplies.

An intricate network of underground tunnels — which included an electric railway system — could quickly transfer soldiers and supplies where they would be most needed. Inter-bunker telephone and electric lines included failover connections to withstand German sabotage.[7]

Surrounding the bunkers were anti-tank ditches, metal obstacles, mines, and small turrets deigned to slow any invasion and give the military time to reinforce its other defenses.

The line was like "a battleship built on land," according to General Sir Alan Brooke, a British corps commander who visited the Maginot Line in 1939 and 1940.[8] In his diary, he called it "a masterpiece in its way" and "a stroke of genius."[9]

Impressed as he was, Brooke could not help worrying that France had neglected other parts of its military buildup.

"I consider that the French would have done better to invest the money in the shape of mobile defences such as more and better aircraft and more heavy armored divisions rather than to sink all this money into the ground," he wrote in his diary.

The line's "most dangerous aspect," he wrote later, "is the psychological one, a false sense of security is engendered, a feeling of sitting behind an impregnable iron fence…"[10]

The entry would prove eerily correct.

Indeed, French commanders assumed that, based on their experience in the First World War, the line would give them time to build, test, and produce new advanced weapons if Germany attacked again.[11]

The Maginot Line performed superbly in direct assaults, holding off and even repelling several attacks. Unfortunately, those attacks were an anticlimax — other divisions of the German army were already marching on Paris. Using lightning-fast blitzkrieg tactics, the army had invaded through Belgium, largely sidestepping the Maginot Line.

The French military, which had diverted much of its budget to the line, could not mount an effective defense.

[4] William Allcorn. "The Maginot Line 1928-45." August 2003.
[5] Modern Mechanics and Inventions. "France Builds World's Greatest Defense System." March 1931.
[6] J.E. Kaufmann, H.W. Kaufmann, et al. "The Maginot Line: History and Guide." 2011.
[7] Ibid.
[8] Alan Brooke (writing as Field Marshal Lord Alanbrooke); Alex Danchev and Daniel Todman (editors). "War Diaries 1939-1945." June 2003.
[9] Ibid.
[10] Ibid.
[11] J.E. Kaufmann, H.W. Kaufmann, et al. "The Maginot Line: History and Guide." 2011.

Using data gathered from more than 1,200 real-world FireEye deployments, this paper explains how attackers are changing tactics, why traditional defenses and testing procedures fall short — and what it means for organizations that rely on them to protect intellectual property, customer data, and more.

Cybersecurity's Maginot Line

Cybersecurity faces a similar transformation. Yesterday's broad scattershot attacks have given way to organized attacks funded by deep-pocketed threat actors who are laser-focused on breaching systems and stealing data.

But like generals still fighting the last war, much of the industry remains stuck in an earlier era. Even as threat actors invent clever new ways to achieve their mission, traditional security vendors, testing bodies and the organizations that rely on them have fixed their gaze on yesterday's tactics. As a result, they leave themselves exposed to new highly effective tactics of advanced threat actors.

In cybersecurity, as in war, even the best-laid battle plans can fall apart in the face of a creative and powerful adversary. The only true test of a product is in a real-world setting.

A view from the front

FireEye is uniquely situated to provide that real-world assessment. FireEye network and email appliances sit behind all other conventional security measures.[12] This means attacks detected by FireEye in these tests have bypassed all of an organization's other security layers.

Using data gathered from more than 1,200 real-world FireEye deployments, this paper explains how attackers are changing tactics, why traditional defenses and testing procedures fall short — and what it means for organizations that rely on them to protect intellectual property, customer data, and more.

Real-World Testing

Laboratory testing is inherently flawed. It can only gauge the effectiveness of cyber defenses against threats that are preselected — and therefore known — by the tester. In addition, testing methodologies often reflect faulty assumptions about how real-world attacks unfold. As a result, technologies that seem effective in a controlled lab setting can fail against unpredictable real-world threats.

To more accurately gauge the effectiveness of conventional security measures, FireEye analyzed real-time data generated automatically by 1,614 appliances in proof-of-value (PoV) trials among 1,216 organizations across the globe from October 2013 to March 2014. These organizations were testing FireEye network and email appliances but not yet protected by the FireEye platform. This setting offered a unique glimpse into how well traditional security products perform in real-world networks.

---

[12]FireEye appliances powered by the patented Multi-Vector Virtual Execution (MVX) engine, monitor Web and email traffic that has passed through firewalls, intrusion detection and prevention systems (IDS/IPS), and Web proxies. Rather than relying on binary signatures, the MVX engine analyzes suspicious files and objects executed within a virtual machine environment. So it detects malicious activity that other defense-in-depth layers miss. FireEye appliances also identify command-and-control traffic from malware not stopped by endpoint tools
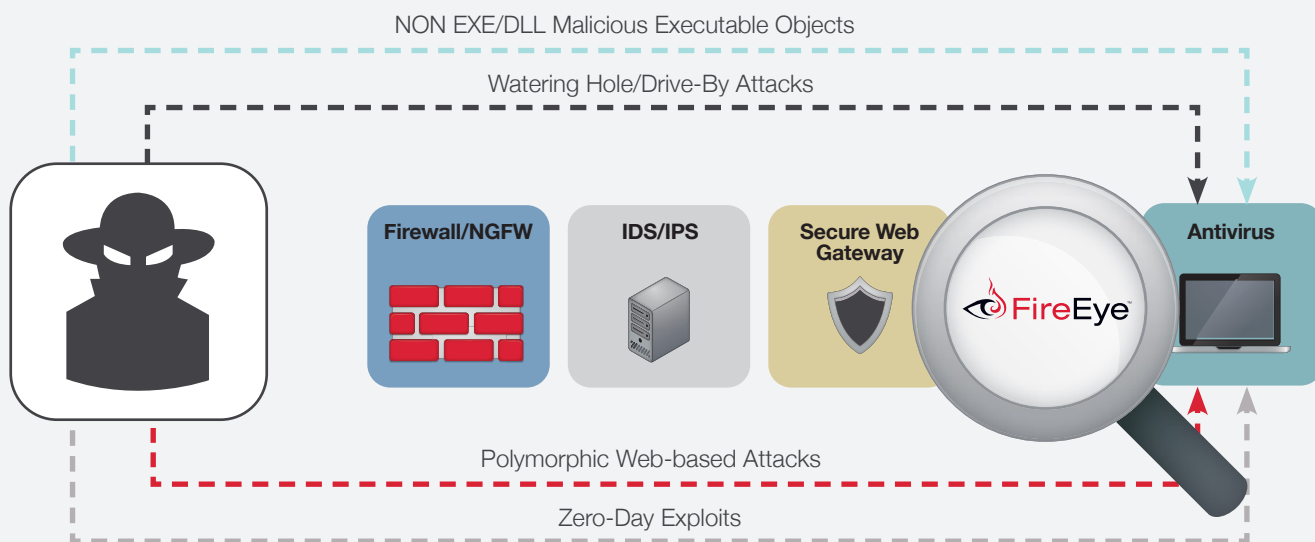
Figure 2: Where FireEye sits in the typical defense-in-depth architecture.

As illustrated in [Figure 2], FireEye network and email appliances typically operate behind other security measures. Anything detected by a FireEye appliance, by definition, has passed through all other layers of a defense-in-depth architecture. By monitoring outbound command-and-control (CnC) attempts that went undetected by anti-virus (AV) we were also able to assess AV and other endpoint defenses in these real-world tests.

FireEye analyzed real-time data generated automatically by 1,614 appliances in proof-of-value (PoV) trials among 1,216 organizations across the globe from October 2013 to March 2014.

Tested Organizations by Geography
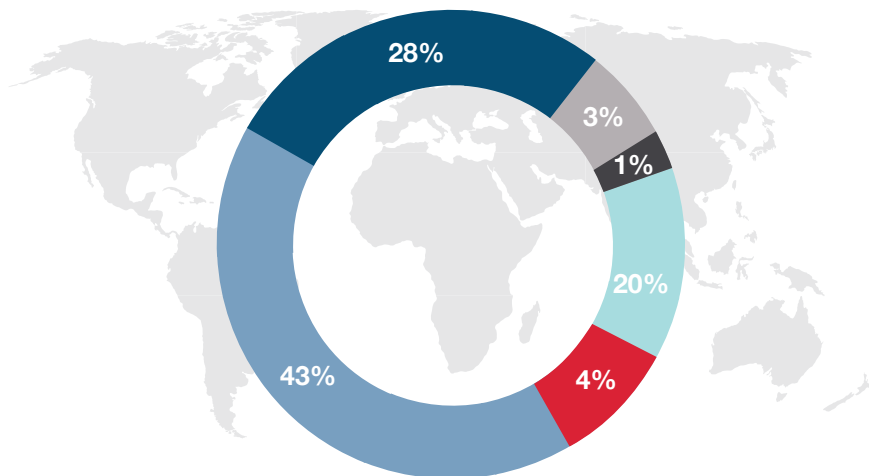
	North America	528	(43%)
	Latin America	38	(3%)
	Europe, Middle East, and Africa	351	(29%)
	Asia Pacific	242	(20%)
	Japan	54	(4%)
	Rest of the World:	3	(less than 1%)

Table 1: The top eight industries represented by concentration.

Industry	% of Total
Financial Services	18%
Government	16%
Chemicals and Manufacturing	7%
High-Tech	7%
Consulting	7%
Energy	6%
Retail	5%
Healthcare	4%

Diverse geographies and industries

Our sample included results from every region in the world and spanned every major industry. As a result, it reflects a broad range of attackers, techniques, and motives that cannot be replicated in a lab environment.

Deep-dive interviews

In addition to the auto-generated data, we surveyed 348 organizations in our sample to better understand the rest of their cybersecurity infrastructure and get additional context about each component of their existing defense-in-depth architecture.

The implication is clear: no corner of the world is remote enough to avoid falling into attackers' crosshairs, and current defenses are stopping virtually none of them.

FACTS FROM THE FRONTLINES:
TEST RESULTS

For this report, we analyzed the data generated from the 1,217[13] FireEye trial deployments for insight into inbound activity (exploits and binaries) and outbound activity (CnC callbacks). By correlating the survey responses with data generated from those respondents' FireEye appliances, we could gauge how effective each defense layer performed in a real-world environment.

Inbound exploits and binaries

Over the six-month test period we observed the following:

Three-fourths of the systems observed in our tests had active CnC sessions taking place. These systems weren't just compromised; they were being actively used by an attacker for activities that could include exfiltrating data.

The implication is clear: no corner of the world is remote enough to avoid falling into attackers' crosshairs, and current defenses are stopping virtually none of them.

In all, the security tools in our tests allowed 208,184 malware downloads. Of those, 124,289 were unique malware variants.[14] Of those unique variants, 75 percent were detected in only one

97%
of organizations were breached

27%
of organizations experienced events known to be consistent with tools and tactics used by advanced persistent threat (APT) actors.

122
On average, 1.6 exploits and 122 malware droppers passed through other security layers.

[13] One of the 1,216 customers cited earlier tested two FireEye deployments.
[14] Multiple binaries of the same malware variant obfuscated with executable compression tools (also known as binary packers) were counted only once.

environment. This finding reflects the growing flood of unique binaries and suggests that many of them were custom made for a particular attack.

Outbound CnC calls

Three-fourths of the systems observed in our tests had active CnC sessions taking place. These systems weren't just compromised; they were being actively used by an attacker for activities that could include exfiltrating data.

We saw 10,149,477 CnC transmissions over the six-month test period to 35,415 unique CnC infrastructures, or 360,965 per week.

The CnC traffic flowed just about everywhere in the world, according to first-stage CnC connections logged during our tests. The first-stage CnC server doesn't always point to the source of the attack — many attackers use compromised machines or buy

infrastructure in other countries to carry out campaigns. But the number and variety of IP addresses shows the global nature of the problem.

The U.S. is far and away the top destination for CnC traffic in the world. This ranking is likely due to the country's large and pervasive computer culture and the number of attractive targets.

Based on our data, these industry verticals had the highest number of malware callbacks from within their network infrastructures:

1. Higher education
2. Financial services
3. Federal government
4. State and local government
5. High-tech
6. Telecom (including Internet)
7. Chemicals/Manufacturing/Mining
8. Services/Consulting
9. Energy/Utilities/Petroleum
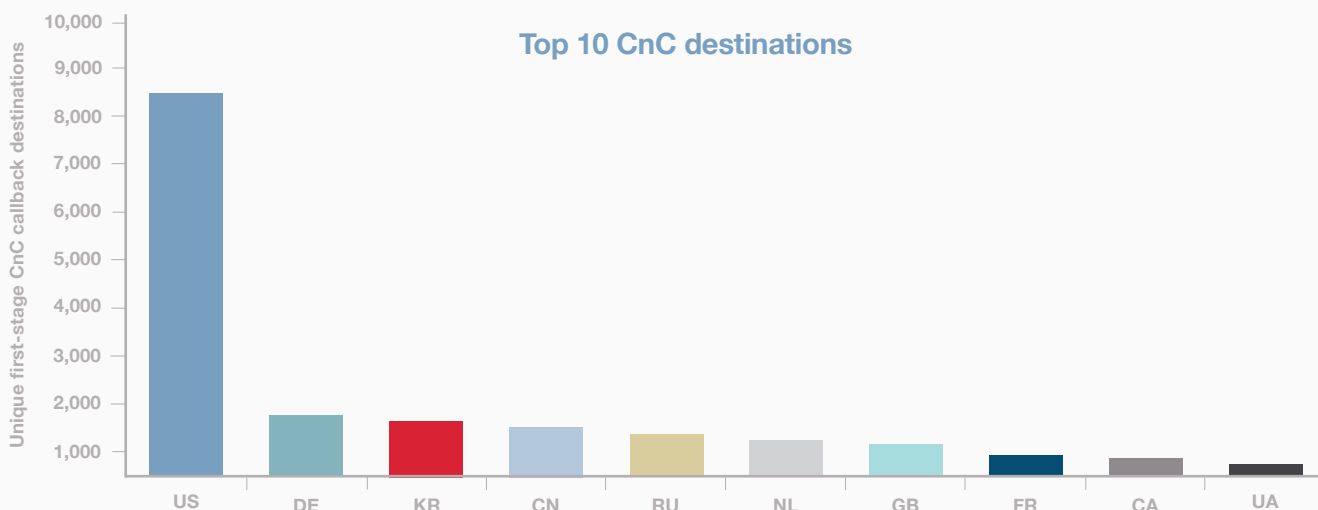10. Healthcare/Pharmaceuticals

Top 10 CnC destinations

Figure 3: First-stage CnC volume. The U.S. is far and away the top destination for CnC traffic in the world.

Education's top ranking is consistent with the 2013 FireEye Advanced Threat Report, which showed that this vertical is frequently targeted. Schools' enticing combination of valuable intellectual property and open network philosophy likely make them prime targets.

Peeling the onion, layer by layer

Isolating the performance of each component of the typical defense-in-depth architecture, we found across-the-board failure — even when multiple layers were working together. Analyzed individually, the most common types of conventional security products experienced at least one breach, leaving systems exposed during our short test period.

We assessed anti-virus tools, which sit below FireEye appliances in most security architectures, by monitoring CnC connections generated by malware that went undetected by AV.

> Not surprisingly, each layer was heavily represented by the best-known names in cybersecurity. We saw no correlation between efficacy and vendor market share — all of the tools failed.
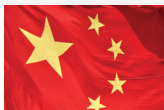
Of the more than 120,000 malware samples identified in our real-world data, more than half had been cataloged in VirusTotal, an online malware repository used by security researchers. Even so, the majority of the AV vendors (the top six) missed 62% of the malware at the time of FireEye detection. And a fourth of the malware wasn't detected by any of those vendors.

Not surprisingly, each layer was heavily represented by the best-known names in cybersecurity. We saw no correlation between efficacy and vendor market share — all of the tools failed.

Table 2: Performance of Defense-In-Depth Security Architecture

Component	Customers That Reporting Using This Security Measure	Breach Rate
Firewall	212	100%
IDS/IPS	119	100%
Web proxy	138	100%
Network anti-virus	75	100%
Endpoint AV	169	100%
Other anti-malware	33	100%

Vendor distribution in customer surveys

Firewall	Network AV	IDS/IPS	Web Proxy	Endpoint AV

Firewall		Network AV		IDS/IPS		Web Proxy		Endpoint AV	
Vendor A	32%	Vendor A	28%	Vendor A	15%	Vendor A	26%	Vendor A	32%
Vendor B	24%	Vendor B	26%	Vendor B	14%	Vendor B	21%	Vendor B	24%
Vendor C	12%	Vendor C	7%	Vendor C	14%	Vendor C	14%	Vendor C	10%
Vendor D	12%	Vendor D	6%	Vendor D	13%	Vendor D	7%	Vendor D	11%
Vendor E	9%	Vendor E	5%	Vendor E	10%	Vendor E	6%	Vendor E	9%
Other	11%	Other	28%	Other	48%	Other	26%	Other	14%

Data Theft: Take Everything but the Kitchen Sink
(excerpted from Mandiant "M-Trends® 2014: Beyond the Breach")

When Mandiant responds to an incident, the first question clients often ask is "why am I a target?" That's often followed by "I don't have anything that anyone would want."

Our answer, borne out through many investigations over the past few years, is increasingly, "yes, you do!" Some nation state threat actors are expanding the scope of their cyber operations. For example, China-

based advanced threat actors are keen to acquire data about how businesses operate — not just about how they make their products.

We have written in past M-Trends reports that China-based threat actors have expanded their targeting well beyond the defense industrial base. Across numerous industries, we've increasingly observed the Chinese government conduct

expansive intrusion campaigns to obtain information to support state-owned enterprises.

This translates into data theft that goes far beyond the core intellectual property of a company, to include information about how these businesses work and how executives and key figures make decisions.

What Today's Attacks Look Like

As these results show, today's attackers have evolved their tactics from just a few years ago. Broad, opportunistic, scattershot attacks designed for mischief have been eclipsed by sophisticated attacks that are advanced, targeted, stealthy, and persistent.

This new generation of attacks includes high-end cybercrime and state-sponsored campaigns known as advanced persistent threat (APT) attacks. Although their aims differ, both types of attacks share several key traits.

All attacks involve a human attacker

All cyber attacks involve a human adversary. In many cases they can involve groups of people under the same organizational umbrella, with multiple teams of people assigned to specific tasks as part of a common mission.[15]

Because attackers are living, breathing people — not pieces of mindless code — they are motivated, organized, and unpredictable.

Today's attacks unfold in stages

Cyber attacks are not a single event. They unfold in multiple coordinated stages, with calculated steps to get in, establish a foothold, surveil the victim's network and steal data.

Here's how a typical attack plays out:

1. **External reconnaissance.** Attackers typically seek out and analyze potential targets — anyone from senior leaders to administrative staff — to identify persons of interest and tailor their tactics to gain access to target systems. Attackers can even collect personal information from public websites to write convincing spear-phishing email.

2. **Initial compromise.** In this stage, the attacker gains access to the system. The attacker can use a variety of methods, including well-crafted spear-phishing emails and watering-hole attacks that compromise websites known to draw a sought-after audience.

3. **Foothold established.** The attackers attempt to obtain domain administrative credentials (usually in encrypted form) from the targeted company and transfer them out of the network. To strengthen their position in the compromised network, intruders often use stealthy malware that avoids detection by host-based and network-based safeguards. For example, the malware may install with system-level privileges by injecting itself into legitimate processes, modifying the registry, or hijacking scheduled services.

4. **Internal reconnaissance.** In this step, attackers collect information on surrounding infrastructure, trust relationships, and the Windows domain structure. The goal: move laterally within the compromised network to identify valuable data. During this phase attackers typically deploy additional backdoors so they can regain access to a network if they are detected.

5. **Mission completed?** Once attackers secure a foothold and locate valuable information, they exfiltrate data such as emails, attachments, and files residing on user workstations and file servers. Attackers typically try to retain control of compromised systems, poised to steal the next set of valuable data they come across. To maintain a presence, they often try to cover their tracks to avoid detection.

---

[15] Mandiant. "APT1: Exposing One of China's Cyber Espionage Units." February 2013.

Today's attacks exploit multiple threat vectors

Advanced attacks cut across multiple threat vectors. For example, a phishing email might contain a link to a malicious URL. In another example, a targeted attack in 2013 against a U.S.-based financial institution used a remote administration tool (RAT) that included both Windows and Android components to spy on victims through PCs and phones.[16]

Many attacks are also multi-flow. Rather than sending a single malicious file to a targeted system — where it might trigger a malware alert— attackers send several files or objects that appear harmless by themselves. When combined, these files and objects reveal their true nature.

For instance, many Web-based attacks comprise multiple downloaded files or objects. These objects often stem from multiple HTTP request and responses, including redirects, and multiple TCP sessions.

One object might be used for a heap spray. Another object might include a buffer overflow or un-sanitized input to exploit. Another object might defeat OS protections such as address space layout randomization (ASLR) and data execution prevention (DEP). And finally, another downloaded binary might be an image with hidden malicious code that executes only when extracted by another seemingly benign file.

Today's attacks are stealthy

Today's attacks use a variety of stealthy tactics to evade detection and maintain control of compromised systems.

Here are just a few of the techniques attackers use to stay under the radar:

- **Process injection.** As the name implies, this technique involves inserting malicious code into an otherwise benign process. By hijacking a legitimate code, attackers disguise the source of the malicious behavior and evade firewalls and other process-focused security tools.

- **Process camouflage.** In this approach, attackers give their malicious file or object a benign-looking name or one deceptively similar to a known system process or other common process. Svchost.exe and Spoolsv.exe are often spoofed because several copies of these services are typically running and can be easily overlooked.
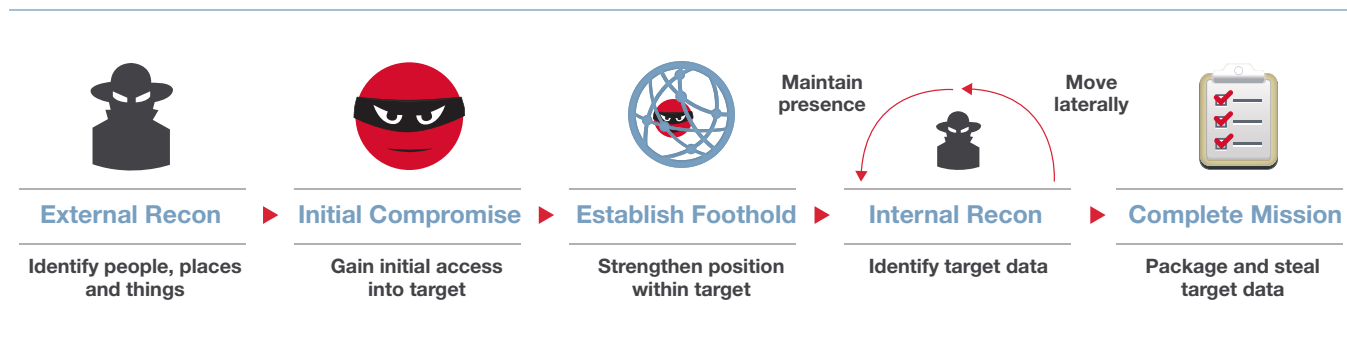

External Recon	Initial Compromise	Establish Foothold	Internal Recon	Complete Mission
Identify people, places and things	Gain initial access into target	Strengthen position within target	Identify target data	Package and steal target data

Figure 4: Stages of an advanced attack.

---

16   Thoufique Haq, Hitesh Dharmdasani, et al. (FireEye). "From Windows to Droids: An Insight in to Multi-vector Attack Mechanisms in RATs." March 2014.
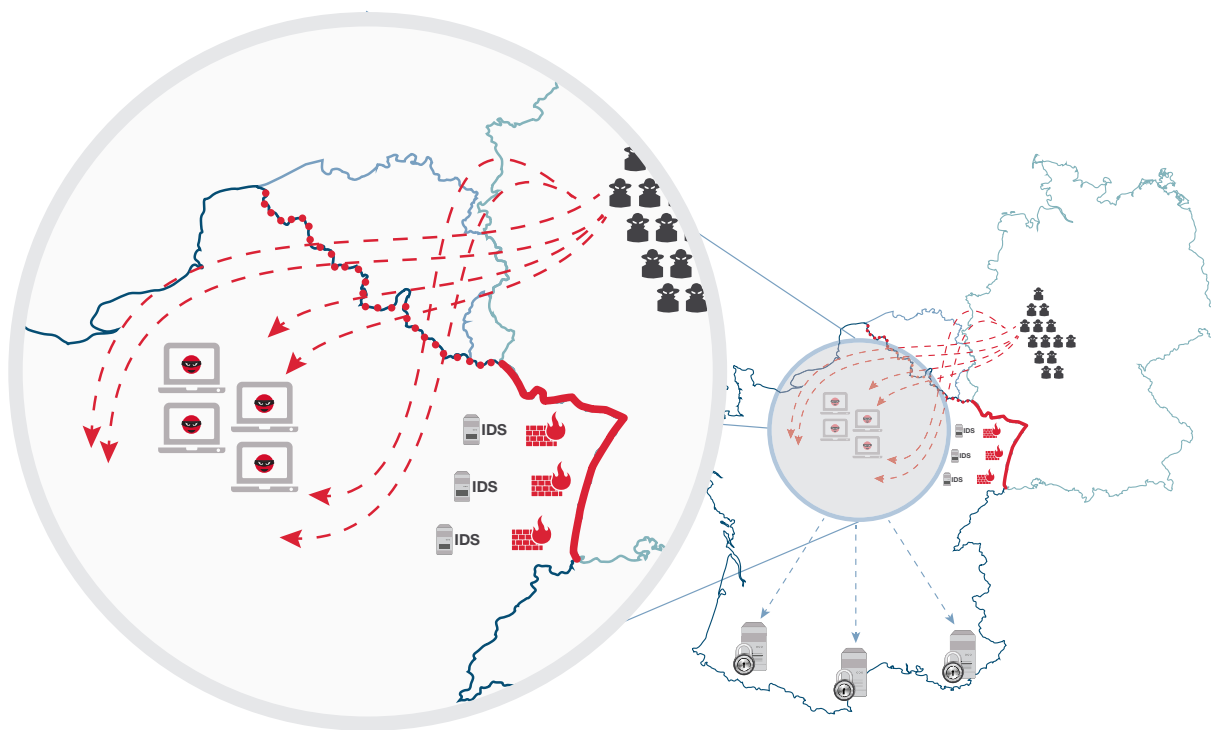
Figure 5: How today's advanced cyber attacks match up against conventional IT defense.

Characteristics of today's advanced attacks and attempted countermeasures of the typical defense-in-depth architecture

Professional Targeted Attacks	Common IT Security Defense
Agile, rapid methods	Signature based
Tools and techniques modified to avoid signature defense	Impervious to repeat attacks using methods that match signatures
Persistent, full-time, paid attackers	Majority spend in most security budgets

- **Executing code from memory.** By running only in memory, malicious code can evade malware scans and leaves no trace of itself for digital forensics investigators. This technique was a key part of Operation Ephemeral Hydra, a sophisticated watering-hole attack discovered in November 2013.[17]

- **File hiding.** This technique can be as simple as altering the timestamp of a file to disguise its creation time in relation to a breach.

- **Trojanizing.** To avoid leaving behind a telltale executable file, many attacks instead hijack an existing executable. Security experts often overlook these files.

Trojanizing a binary that is loaded on system boot offers the added benefit of persistence.

- **Packers.** Packers compress and encrypt code to hide the underlying code. The technique creates new binaries that have not yet been identified by signature-based cyber defenses. It also makes reverse-engineering code more difficult.

---

[17] Ned Moran, et al (FireEye). "Operation Ephemeral Hydra: IE Zero-Day Linked to DeputyDog Uses Diskless Method." November 2013.

> As our test results show, the Maginot line of cybersecurity is no match for the determined attackers tasked with stealing corporate secrets.

Many attacks are tailored

Today's attacks often involve malware tailored to compromise a single target. As explained earlier, 75 percent of unique malware in our samples were detected in only one environment. That is consistent with a comprehensive FireEye analysis of 2013 attacks, which found that 82 percent of malware binaries disappear within an hour. No wonder an executive at AV software giant Symantec recent declared the technology "dead."[18]

When attackers make the effort to customize an attack for a specific target, they tend to continue attacking until they have achieved their objective.

The New Maginot Line

As our test results show, the Maginot line of cybersecurity is no match for the determined attackers tasked with stealing corporate secrets.

How today's architecture falls short

Today's typical defense-in-depth architecture comprises several discrete layers, including anti-virus software, intrusion-prevention systems (IPS), so-called "next-generation" firewalls, and Web gateways. As our real-world data makes clear, this framework is poorly equipped to combat today's advanced attacks.

First, the individual components are designed to manage a single piece of the security puzzle and are usually not well integrated. An organization may think that it has covered all of the major threat vectors. But without a complete, cohesive view across all attack vectors, today's defense-in-depth model can miss the signs that an attacker has breached their defenses.

A bigger problem is foundational. Most components in the typical security architecture rely on a mix of binary signatures, blacklists, and reputation to identify threats. These approaches might have held off an earlier generation of attacks. But like France's Maginot Line, they are no match against today's threats.

Signatures are ineffective because AV vendors cannot keep up with the deluge of new malware binaries. In many cases, the malware is custom-made for the target, meaning AV vendors will never see it — let alone create a signature for it. Many attacks also exploit zero-day vulnerabilities, which by definition are unknown.

Application blacklists are blind to attacks that use encrypted binaries or hijack legitimate apps and processes. Often, the initial exploit is not an executable file at all. Other reputation based defenses, like those used in Web gateways and IPS, cannot stop attacks from newly minted URLs or compromised websites serving up drive-by-downloads.

Even sandboxing technology, hailed as a great leap forward for cybersecurity, is flawed in most implementations (see sidebar).

---

[18] Danny Yadron (The Wall Street Journal). "Symantec Develops New Attack on Cyberhacking." May 2014.

Thinking Outside the Sandbox

In a grudging admission that traditional security tools are no longer working, security vendors are scrambling to add dynamic analysis tools, also known as sandboxes, to their portfolio. Even incumbent vendors who have long defended their aging legacy tools have embraced the concept.

Sandboxing remains a nascent technology, and only a handful of the systems in our sample had deployed one. But even in this small set the trend was clear. Every single system with a sandbox was breached.

What is sandboxing?

Instead of relying on signatures, automated dynamic analysis systems observe malware behavior using off the shelf virtual machines (VMs). These walled-off, simulated computer environments allow files to execute without doing any real damage.

By watching the files in these virtual sandbox environments, automated analysis systems can flag telltale behavior, such as changes to the operating system or calls to the attacker's CnC servers.

Why most fall short

Many sandboxes are easily detected and evaded. Some analyze files in isolation rather than as part of a coordinated whole. Some myopically focus on a single threat vector. Some fail to emulate complete systems or emulate only a single "golden" image. Some measure only the beginning and end states of a virtual system — missing everything that happens in between.

What to look for in dynamic analysis

To truly protect IT assets, virtual-machine-based analysis must overcome the sandbox-evasion techniques of advanced malware. And when new evasion techniques emerge, vendors must quickly update their tools.

As explained earlier, today's attacks unfold over multiple vectors and multiple data flows. They unfold in multiple coordinated stages, with calculated steps to get in, establish a foothold, surveil the victim's network and steal data.

That means dynamic analysis must analyze files and objects in context and across multiple threat vectors. And they must offer a wide variety of environments to detect targeted malware.

Virtual-machine-based analysis is even more effective when augmented by dynamic, real-time threat intelligence and a full complement of services. With a complete view of attacks within an enterprise, geography, or industry, security teams can better prevent, detect, contain, and resolve advanced attacks.

CONCLUSION AND RECOMMENDATIONS

Despite the billions of dollars organizations pour into traditional security measures every year, attackers are compromising organizations almost at will.

As our data shows, it doesn't matter what vendor or combination of typical defense-in-depth tools an organization has invested in. And it doesn't matter how well these tools performed in lab tests. Real-world attackers are bypassing them all.

Brooke, the British General who found the Maginot Line so impressive during his visits before the German invasion, privately worried about the French strategy. He feared, correctly, that the country was spending too much on the bunker defenses and too little on modern equipment and weapons that could adapt to the vagaries of war.

In our tests, attackers got through organizations' cyber Maginot line at least 97 percent of the time. They compromised more than 1,100 critical systems spanning a wide gamut of geographies and industries. This suggests that thousands upon thousands of organizations around the world may be breached and not even know it.

"Millions of money stuck in the ground for a purely static defence," he wrote after one visit to a Maginot bunker. "The total firepower developed by these works bears no relation to the time, work and money spent on their construction."[19]

Many organizations may be making the same mistake. In our tests, attackers got through organizations' cyber Maginot line at least 97 percent of the time. They compromised more than 1,100 critical systems spanning a wide gamut of geographies and industries. This suggests that thousands upon thousands of organizations around the world may be breached and not even know it.

In light of this reality, organizations must consider a new approach to securing their IT assets. For many, that shift should include reducing waste on redundant, backward-looking technology and redeploying those resources on defenses designed to find and stop today's advanced attacks.

19   Alan Brooke (writing as Field Marshal Lord Alanbrooke); Alex Danchev and Daniel Todman (editors). "War Diaries 1939-1945." June 2003.
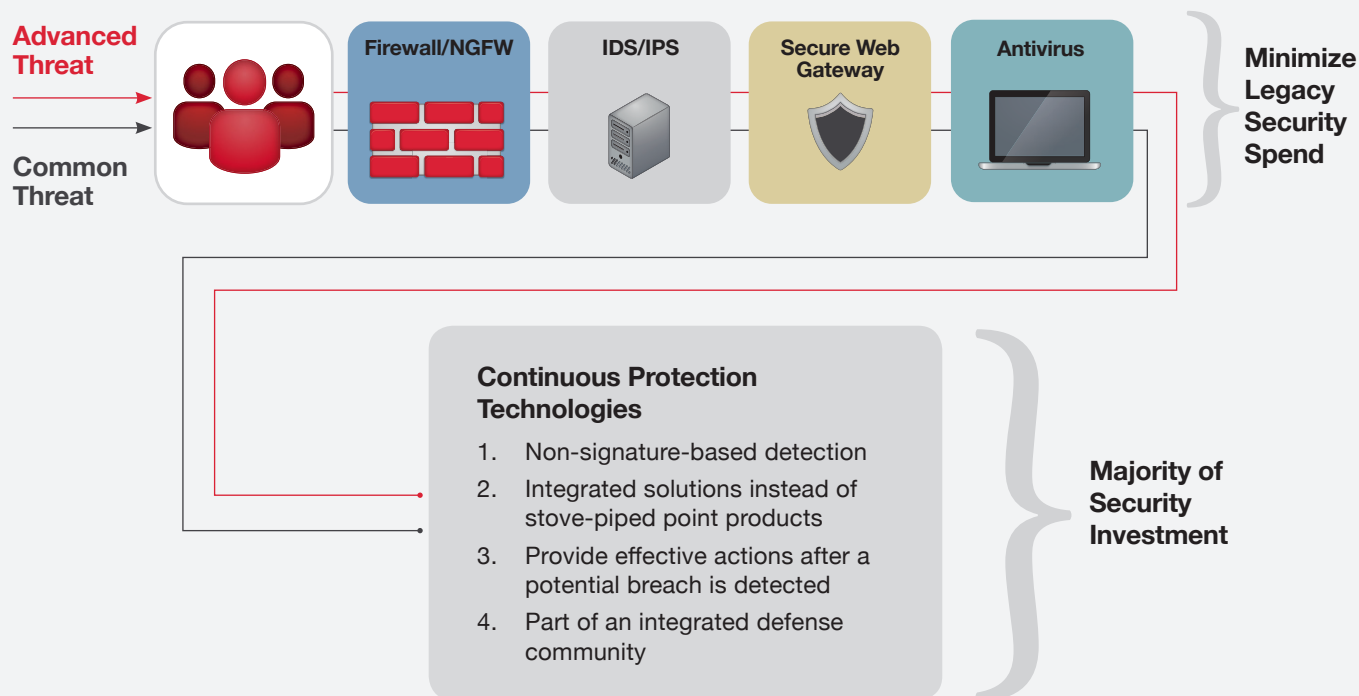
Figure 6: Organizations should consider reducing waste on redundant, backward-looking technology and redeploying those resources on defenses designed to find and stop today's advanced attacks.

FireEye recommends the following:

Evolve

to a different architecture that is not based on signatures, whitelists, or reputations. Instead, deploy VM-based security solutions that provide full attack coverage and generate high-quality, accurate alerts so you can see the alerts that matter.

Invest

in rapid endpoint-response capabilities to validate and contain attacks that get through.

Build

(or hire) an incident-response capability to respond when necessary.

Reduce

redundant signature-based defense-in-depth layers that don't catch threats and create extra noise. Reinvest those resources in effective VM-based security solutions.

FireEye helps organizations defend themselves against the newest generation of cyber attacks. The combination of our threat prevention platforms, people and intelligence helps eliminate the consequences of security breaches by detecting attacks as they happen, communicating the risk, and equipping you to rapidly resolve security incidents.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393)
info@FireEye.com | www.FireEye.com