Aite PARTNER. ADVISOR. CATALYST.

Ransomware Defense in Financial Services: Retreating From the Cloud

This report excerpt has been provided compliments of:

AUGUST 2020

Steve Hunt

TABLE OF CONTENTS

LIST OF TABLES

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

IMPACT POINTS

- This report is intended to help business and IT executives within large and small financial institutions to understand trends around ransomware and its defense. The report surveys classes of ransomware defenses for small and large organizations, respectively, and describes the trend by financial institutions to rely less on cloud-based endpoint protections and more on smart agent software.
- Aite Group spoke with 11 information security executives representing midsize financial services organizations and several of the largest banks in the world. We also spoke to 16 vendors of defensive technologies and a sampling of their customers. Each vendor profiled has made major changes in its offering or has received significant capital investment in the last 12 months.
- Ransomware attacks can hit any business, and ransoms can exceed US$1 million. Preparation is key, and it involves layered defenses in and around mobile devices, workstations, and servers.
- Antivirus software, secure email gateways, and container or sandbox technologies are table stakes. No company, no matter how small, should be without all three.
- Solutions that rely on machine learning (ML), artificial intelligence (AI), and the cloud simply are not fast enough to respond to the more aggressive ransomware attacks. Instead, the savviest security teams in financial services lean toward faster whitelisting and enforcing policy in memory on workstations and servers.
- Broad, comprehensive suites of ransomware solutions sound attractive to financial institutions with large, complex environments but still require tremendous integration and support. Other vendors offer lighter point solutions that may be mixed and matched for small and midsize organizations with less complex infrastructures.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

INTRODUCTION

There are two kinds of organizations: those that have endured a ransomware attack and those that likely will. In each case, weathering the storm is a matter of preparation, which, as in most things, is easier said than done. Here's why: There is no single technology that prevents ransomware, and there are many kinds of ransomware attacks. Most ransomware attacks enter through emails in the form of malicious links (Proofpoint reports this number to be about 93%). Unfortunately, we cannot infer from that number that we can be 93% more secure by securing email. It's more like playing slots in Las Vegas—the ninety-third pull of the handle has not changed the odds that the next one will spin all cherries. Every pull has the same odds, and every clicked link has equal potential to take down the house. It just takes one click.

And it's getting expensive! In June 2020, The University of California, San Francisco, confirmed that it paid US$1.14 million to a ransomware group.[1] Clicking on malicious links is part of the problem, yet more and more attackers are using ransomware as a final step in multistaged attacks. If attackers target a firm and begin snooping around, they may be successful moving laterally in and around servers and workstations for hours, days, or even months before enough security anomalies trigger a response. When attackers sense that their access is getting cut and their free ride is ending abruptly, that's when they detonate ransomware. Like a car thief torching a car after stripping it of everything valuable, ransomware wipes out almost all traces of its attack. Defense, then, requires layers. This report explores some of the most critical defenses an organization can put in place.

METHODOLOGY

To understand the most current thinking about ransomware defense from the point of view of financial services chief security officers, Aite Group spoke with 11 security executives representing midsize financial services organizations and several of the largest banks in the world. Vendors profiled in this report specialize in ransomware defense and range from young startups to the largest tech firms in the world. We selected a mix of vendors that can be used independently of one another or in concert. The vendors fill three categories of protection:

- Secure email gateways and security containers
- Incident response and analytics
- Detection and response for endpoints and servers

Security awareness training, next-generation firewalls, web application firewalls, backup solutions, multifactor authentication, deception technologies, and automated patching systems are all important parts of a security posture. This report deals with defenses in and around endpoints along with the apps and data on endpoints, and not infrastructure around authentication and access.

1. "Update on IT Security Incident at UCSF," UCSF Campus News, June 26, 2020, accessed August 12, 2020, https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

THE MARKET

Researchers in the industry and Aite Group report similar trends: Ransomware is a particularly knotty problem, it's growing in scope and scale, and it's getting more expensive (Table A).

Table A: The Market

Market trends	Market implications
Most organizations have seen an increase in cyberattacks during the pandemic.	Ninety-six percent of IT executives surveyed by Tanium in July 2020 said they plan to make changes to reduce risk as employees return to offices. They'll do this primarily by investing in endpoint management along with other technologies.[2]
Targeted ransomware is on the rise.	Broadcom's Symantec research team reports that targeted ransomware attacks increased 30%, while nontargeted "spray and pray" ransomware dropped 20% in recent months.[3]
Malware is 30 times more damaging than a data breach.	According to IBM, US$239 million is the average cost of a destructive malware incident in 2019, which is almost 30 times the cost of a data breach.
Ransoms reached US$1 million.	In June 2020, The University of California, San Francisco, announced that it paid US$1.14 million to a ransomware group.
Large organizations should expect a US$200 million impact from ransomware.	IBM X-Force Incident Response and Intelligence Services (IRIS) estimates that in 2020, victimized organizations on average experience a total cost of over US$200 million and have more than 12,000 devices destroyed in an attack.[4]
Phishing is still effective.	The Verizon Data Breach Investigations Report 2020 reported that more than 80% of financial services organizations surveyed suffered loss from phishing.[5]
Cloud solutions are held at arm's length.	IT executives interviewed by Aite Group were unanimously wary of cloud-based protections for endpoint devices.

Source: Aite Group, Tanium, Broadcom, IBM X-Force, Verizon Data Breach Investigations Report 2020

2. "Tanium Report Reveals 90 Percent of Organizations Experienced an Increase in Cyberattacks due to COVID-19," July 29, 2020, accessed August 12, 2020, https://www.tanium.com/press-releases/tanium-report-reveals-90-percent-of-organizations-experienced-an-increase-in-cyberattacks-due-to-covid-19/.

3. Data provided by Broadcom analyst relations.

4. Data provided by IBM analyst relations.

5. "2020 Data Breach Investigations Report," Verizon, accessed August 12, 2020, https://enterprise.verizon.com/resources/reports/dbir/.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

TRENDS

Aite group's conversations with 16 vendors and 11 security executives at midsize and large financial institutions revealed that banks tend to value prevention over detection and on-premises over cloud-based:

- Ransomware is indiscriminate, targeting every company of every size. Ransomware employs a variety of tactics, from phishing emails to multistaged attacks.
- Cloud-based solutions for threat analysis are popular, while cloud-based protection and mitigation are held suspect. Ransomware simulates normal behavior, so any attempt to stop malicious behavior risks interrupting normal behavior. ML and AI in the cloud are a good way to get more human and robotic eyeballs on the problem to discern whether the normal-looking behavior is malicious. Unfortunately, it is slow. Therefore, vendors with real-time detection and prevention solutions are gaining momentum over cloud-dependent and ML-dependent solutions among financial service organizations.
- Ransomware defense is moving away from searching for known malicious code or signature-based blacklisting. Instead, vendors with the ability to catalog known good behaviors and detect deviations and that can do it in real time on workstations and servers are the fastest and most reliable protections. This technique, known as whitelisting, is popular for its ability to detect and stop malicious activity quickly without relying on analysis in the cloud.
- Defensive techniques depend on layering defenses in such a way as to identify and stop malicious behavior before it goes too far. Vendors typically sell one or more of these layers, with the most comprehensive solutions coming from vendors that package together more layers.
- More layers equal more cost and complexity. Smaller businesses tend to cobble together a defense from simple, stand-alone products, while large organizations prefer comprehensive suites.

RANSOMWARE IS HERE TO STAY

Ransomware will take down operations of a hospital, a city hall, a small company or a global enterprise, a shipping company, or a credit union. The victims of ransomware suffer not because they failed to protect themselves—even the most prepared get affected to some extent. Rather, they suffer because the magnitude and speed of ransomware are simply beyond their level of preparation.

Each ransomware attack reported in the news is a reminder to diligently adopt security best practices and take an attitude of adaptation and continual improvement. Ransomware itself is not terribly complicated, but defending against it requires ingenuity. For example, when users click on a link in a phishing email, they launch a chain reaction. The speed of those next steps confounds endpoint defenses that IT professionals have relied on for years, spreading quickly and jumping from one machine to the next.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Imagine water particles in the air, each charged with the COVID-19 virus, infecting dozens of people before the first person shows symptoms. Ransomware is exactly like that. It sprinkles its infected droplets quickly, and those droplets are hard to spot. Identifying ransomware in action is difficult because it is not doing unusual things. It is performing normal operating system functions such as reading files, renaming files, and encrypting files. That's the stuff of everyday business. Therefore, ransomware defense has multiple fronts—filtering and scanning traffic, monitoring behavior, analyzing threats and vulnerabilities, rehearsing incident response, recovering from backups, patching systems, inspecting system calls, etc.

ATTACKERS CAST DIFFERENT LURES

Security faces an uphill battle for respect. If security professionals are very good at keeping bad things from happening, then nothing happens, and it looks like there's no need for security. Measuring risk is another of the dark arts. Quantifying statistical likelihoods and theoretical impacts of security events can make your eyes cross.

When it comes to ransomware and many other threats facing businesses today, the inevitable happens to security professionals again. When they install security software to detect and respond to ransomware threats, suddenly that software detects hundreds of new events that had not been previously tracked, making it appear as if the problem just got worse. When vendors report that numbers of attacks are growing, let's take that with a grain of salt.

However, there is one thing that can be measured well, namely, how the attacks appear to us. Last year, phishing and social engineering threats came in dozens of common formats, according to the Verizon Data Breach Investigation Report 2020. Vacation rental scams, free tickets to the Super Bowl or the World Cup, billing problems with your Netflix account—"click here to log in and make a payment"—and of course, emails from the occasional Nigerian prince are among the most common of 2019.

In March 2020, however, phishing with ransomware payloads transformed to be laser-focused on the topics that are on top of mind of most people, according to anecdotes from large enterprise chief information security officers (CISOs) and reports from Microsoft, Proofpoint, and Cisco. At the beginning of the COVID-19 crisis, employers required people to work from home and scrambled to provide a secure working environment, with the twin objectives of safety and productivity. Outside of financial services, productivity—not security—was the chief motivator. Hackers quickly adapted to take advantage of the crisis. Predictably, ransomware attacks preyed on stress and isolation. Attacks came veiled as COVID-19-themed emails, COVID-19-related financial information, fake World Health Organization messages, phony Centers for Disease Control communications, and many more, urging readers to "click here to receive your government stimulus compensation," and so forth.

Thereafter, organizations that Aite Group spoke with saw a need to layer security controls for the home workers. Those new controls opened new doors for attack.

For example, conversations with large enterprise CISOs and several vendors revealed that many companies established more VPN connections than ever before. To conserve bandwidth, IT managers configured VPNs to use split tunneling, introducing new vulnerabilities, foreign to the

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

internal network of yesterday. That triggered organizations to update users' machines remotely. This presented a new problem, because small and midsize companies commonly use remote assistant services running on the remote desk protocol (RDP) port, a favorite port for hackers and ransomware attacks.

Ransomware attacks continue to grow in numbers of new victims per year and severity of impact. That makes sense, because ransomware is now a big business, generating over US$11 billion for attackers in 2019, according to Cybersecurity Ventures.[6] On the dark web, companies specialize in various nefarious aspects of the attack economy. For example, a few companies sell malware, others sell lists of targets, and still others host the attack with a full suite of customer support features for their customers, who are attackers themselves.

Because of the support available to an attacker and the relatively low threshold of skill required to enter the business, ransomware will continue to grow rapidly, adapting, as any business does, to new environments. Attackers can encrypt or steal data and hold it for ransom and threaten to release that data to the public. Because many companies are willing to pay ransoms, and insurance companies are willing to cover ransom costs, ransomware is not expected to slow down anytime soon. In addition, the ability of the ransomware economy to adapt based on the defenses of its targets makes ransomware defense a very dynamic field.

Ransomware enters an organization most often through email. Clicking on links gets the most results, but other techniques can launch the first stages of an attack by simply enticing a user to hover their mouse over an image or visit a web address. That's the thing—it's not rocket science. Creating and deploying ransomware is built on common vulnerabilities that have been used by bad actors for decades and looks to the defenders like regular activity. Structured query language (SQL) injection looks like regular browser activity, command injection looks like normal applications, deploying malware uses everyday functions such as PowerShell and JavaScript, and encryption is done all the time by applications such as Slack, Excel, and many others.

Where to place defenses, then, varies. Organizations can attempt to repel malicious links, send suspected malicious code and links to a cloud service to be inspected before they execute, inspect the code on an endpoint before it executes, let code execute but perform behavioral analysis and blocking in real time, let the code execute in a virtual container or sandbox, and combinations of each. Ransomware defense is still as much art as it is science. That's why the most protected companies use their own personal combination of technologies. Now you can pick yours.

BASELINE DEFENSES

Every company should have certain basic defenses in place. Large and small organizations can turn to nearly comprehensive suites and somewhat simpler and much less expensive stand-alone solutions. There are, however, some fundamentals every firm must have in place, no

6. Steve Morgan, "Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) by 2021," Cybersecurity Ventures, October 21, 2019, accessed August 19, 2020, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

matter how large or small. Nearly every company has had antivirus software installed since it first installed personal computers, but not every company has other basic defenses such as containers, agents, threat analysis, and in-memory whitelisting.

NEXT-GENERATION ANTIVIRUS

If all computers and companies have antivirus—and it's been installed for the last 20 years—why is ransomware a problem? Why didn't antivirus vendors step up to address the problem? The answer is that ransomware and other "new" threats exploited the biggest weakness in antivirus defense: blacklisting, or making a list of code or signatures that are known to be bad and blocking them.

In the 1990s and early 2000s, threats from the outside came in the form of bits of code that arrived attached to or embedded in email and webpages and the like. New malware was quickly discovered by threat research teams at antivirus vendor "labs" that just as quickly produced a signature update to their product to catch each new bad bug. The update would be pushed out daily to all desktop machines. So, if the lab moved fast enough, the antivirus software on our computers stayed well-informed enough to spot the bad code, block it, and quarantine it before it could wreak havoc.

This was the norm for some time. It was always a race against time, with virus writers working faster and faster to stay ahead of antivirus labs. Things stayed that way until attackers discovered ways of making their attacks more subtle, more persistent, and less identifiable. These so-called advanced persistent threats were soon combined with AI capabilities to morph on the fly, changing into new variants in the field—new variants that signature-based antivirus software simply could not consistently spot.

Today, antivirus vendors employ similar AI as the bad guys to watch the behavior of code as it executes. Code executes fast and may outpace the speed of detection. So, another technology was added to the mix: virtual containers or sandboxes. These "safe" places to run malicious code complement the work of any detection engine, giving the antivirus time to react and block the bad code.

Sandboxes and containers create a temporary artificial space in memory for files to open and code to run. Meanwhile, detection engines watch closely. Combining signatures, AI, and containers in this way is a good way to quiet some of the noise, but antivirus alone is no longer enough for responsible protection.

SECURE EMAIL GATEWAYS AND CONTAINERS

Poor users—they just try to get their work done. They are home-schooling kids, walking the dog, stepping around spouses, and working their day jobs. Work life is new, pressures are different, and threats are real. The chance someone will click that one bad link or fall for that one credential scamming fraud are higher than ever. Knowing this, attackers prey on those pressures by writing phishing emails with promises of stimulus checks, new vaccine information, and news about another coming confinement. Secure email gateways have long been fighting this fight with advanced phishing protections, filtering, and sandboxing (virtual containers for executing code safely).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Detractors say containers are not ideal, because malware can sometimes detect when it is running in a container and will just go to sleep, waking up later when it is in a normal environment. However, containers are still good insurance. While it is critical that organizations put a secure email gateway in place, preferably with sandboxing, and complement next-generation antivirus software with container technologies that execute links in a safe virtual machine, these measures will stop only some attacks.

INCIDENT RESPONSE AND ANALYTICS

When ransomware strikes, there is work to be done. It's not simply a matter of restoring all affected machines from handy backups. First, those backup are rarely so handy. Second, restoring from backups takes time. Lots of time. Multiply that by lots of systems, and backups are a headache. However, before backups are even a consideration, IT staff will be busy addressing first things first—gathering malware samples, documenting the affected domains, and assessing the breadth of attack.

Meanwhile, someone needs to decide whether to pay the ransom or not. There really is no standard on when to pay a ransom or when to accept the attack and its repercussions on the chin. Depending on the damage of the attack, the number of machines affected, the maturity of ransomware defense already in place, and the time estimated to full recovery, paying may be an option. Aite Group sees that insurance carriers generally try to focus on the prevention. If an insured party made every reasonable effort to prevent a cyberattack, cyber insurers are likely to stand behind a claim. IT response teams must still go through the steps of containment and response. These include vaccinating endpoint devices, blocking IP addresses and domains and protocols, resetting passwords, disabling some automatic processes, forensics, and more.

The last step is hardening all systems based on the new knowledge of the attack. Systems will need patches and updates. Networks will need segmentation. And users will need updated training on phishing. If that's not enough, there is even more work to prepare for the next attack, known as pre-incident planning. This is what should have been done in the first place, before any attack took place. But better late than never. Pre-incident planning includes table-top exercises to avoid the "Keystone Cops" confusion that invariably happens when disaster strikes the unprepared.

Vendors profiled in this report approach incident response and analysis in one or two ways: Either they provide powerful software for visibility and rapid analysis, or they provide professional services and advice to jump in and deal with the problem while fires are blazing, or both.

Whether an organization hires a professional team to swoop in and help or go it alone, incident response is only as good as the information at hand. Therefore, the most successful response will have access to extensive, detailed information about incidents, including the precise time, threat ID, victims' and attackers' IP addresses, session tokens, and the full HTTP request that triggered the attack along with the complete attack payload.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ENDPOINT DETECTION AND RESPONSE

The time between attackers gaining access to a network and deploying ransomware has dropped from months or weeks to mere days. So relying only on incident response planning and analysis tools is clearly insufficient. Something must be done to block the offending behavior—and block it fast.

Endpoint detection and response (EDR) refers to software that detects and blocks bad actions on devices such as laptops, desktops, and phones. In an attempt to be clear while wading in the murky waters of marketing speak, EDR is essentially doing what you thought antivirus products were supposed to be doing: stopping malware, detecting malicious activity, and ensuring that the endpoints are configured for appropriate safety.

These solutions rely on software on the endpoint, called an agent, and often refer to a physical server or cloud-based service for deeper analysis of threats and anomalies. The solutions that are more heavily based in the cloud have richer analytical capabilities, and those more heavily weighted on the agent have more prevention strength. Most combine whitelisting (allowing known and trusted applications) and blacklisting (keeping a lookout for known malicious applications). And most also, nowadays, tout some form of AI or ML to aid in detecting and classifying anomalies.

In the last year, most solutions have integrated the popular MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework for classifying methods and tactics of attacks developed by the not-for-profit research and development centers supporting several U.S. government agencies. This framework helps software companies to organize the analysis and recommendations it makes to its customers, and it helps IT security teams to evaluate and respond to incidents more quickly and effectively. Prior to the MITRE framework, security analysts used dark arts and wishful thinking to construct correlations for security incidents. Mercifully, MITRE standardizes analysis.

EDR can be criticized for trying to fit too much into one hard-working software agent. After all, an agent that's always running, always thinking, and always watching, is naturally going to affect performance of a device. These agents are doing several, if not all, of the following functions:

- Threat hunting
- Sandboxing executables
- Preventing exploits on disk
- Preventing exploits in memory
- Detecting anomalous behavior
- Continuously monitoring activity
- Discovering unprotected endpoints
- Blocking certain files and network traffic
- Enforcing custom whitelists and blacklists

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- Communicating with other endpoint agents
- Isolating an endpoint at risk

It's a tall order for any software.

Complexity also puts the full capabilities of EDR software out of reach for small, budget-conscious firms that more commonly will use less expensive and less complex next-generation antivirus plus container software. Larger, more risk-averse enterprises lean toward the full functionality of EDR and the new extended detection and response (XDR).

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

VENDOR PROFILE: VIRSEC

Virsec sells a run-time memory application protection that complements other ransomware defenses. Virsec was launched in 2015 and is headquartered in San Jose, California. The company has 80 employees and serves customers worldwide. About a quarter are financial institutions, and roughly half are in the U.S. The company holds over 30 patents behind its AppMap technology, enabling it to create a whitelist of acceptable files, processes, libraries, web input, memory usage, flow control, and more.

Ransomware is most damaging when it moves laterally from desktops to servers. That's where Virsec Security Platform v2.0 steps in. The product maps in memory the sequence of processes and commands by all applications authorized to run on that server and then waits for any process that differs.

The software monitors processes in memory, and as soon as a foreign application or unknown sequence of functions shows up, the software kills the process and raises an alarm. The product stops unfamiliar sequences of commands, and it stops familiar sequences from unfamiliar sources. In this way, attackers cannot perform command injections to hijack control. It does not have to know every legitimate system call in every app and every context, nor is it learning as it goes. It is simply looking for variations on "normal."

OUR TAKE

Detecting and blocking rogue processes in memory is one of the most important ways to secure servers. Servers are online 24/7/365, unlike workstations, so the opportunity for devastating loss is much higher on servers than on endpoints. Whitelisting the behaviors of normal applications means threat actors won't be successful at introducing any new commands. Even though attackers like to mask their attacks in very normal everyday-looking commands, like READ, WRITE, ENCRYPT, and RENAME, the Virsec product will see through the ruse. Instead of trying to detect a universe of possible attacks, just keep good applications happily purring along.

Virsec is a recommended add-on to Microsoft and Linux servers regardless of the EDR or antivirus protections used on endpoints. It is a suitable stand-alone solution for organizations desiring to upgrade security on critical servers.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

CONCLUSION

A locked vault is better than an alarm system. Financial institutions have always tried to keep valuables behind layers of protection. Today is no different, with banks clearly trending toward having layers of antivirus and real-time protections, rather than merely relying on alarm systems in the cloud. Cloud-based detection solutions have the advantage of data lakes, rich analysis, and ML. And security teams certainly need excellent intelligence to combat aggressive adversaries. But that analysis takes time, which works to the attacker's advantage. Therefore, establish robust protections on endpoints—especially servers—first, before building out detection and response:

- Some protections are optimized for workstations, others, such as Virsec, for servers. When evaluating solutions, consider protecting both.
- Some vendors offer broad one-stop-shop suites for ransomware defense, analysis, and incident remediation across desktops, mobile devices, servers, and cloud services. But each may be enhanced with additional point products. Don't be afraid to layer defenses.
- Others provide detection and prevention agents but are stronger and more specialized in threat hunting, analysis, and incident response.
- Some vendors rely most heavily on cloud-based ML for detection and analysis.
- Virsec is exclusively designed for server protection and is focusing its preventive solutions on real-time memory protection.

Ransomware can be devastating to small and large financial institutions. Strategies for smaller firms start with security-on-a-shoestring and go up from there, increasing both spending and complexity:

- Secure email gateways, next-generation antivirus, and container technology are table stakes. Every financial institution, no matter how small, should have all three. It is better to layer defenses than to rely on a single technology. Therefore, add EDR and other protections on top of antivirus, container technology, and secure email gateways.
- Real-time memory protection on servers is the single most important protection upgrade a company can make.
- Small institutions should consider some firms for foundational protection and a firm such as Virsec as a specialized enhancement.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- Midsize and larger institutions should create a more comprehensive strategy of layered protections:
  - Combine antivirus and EDR
  - Add as much cloud-based analysis as the security team can digest and use
  - Protect servers
- Large institutions should take advantage of security suites complemented by specialized protections.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

RELATED AITE GROUP RESEARCH

Better, Stronger, Cheaper Cybersecurity: Doing More With Less in a Crisis Economy, June 2020.

Advice for CISOs: Help Your Organization Get the Best Results From Cyber Insurance, June 2020.

Making the Case for Identity and Access Upgrades, May 2020.

The Flow of Security, March 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Steve Hunt
+1.617.447.1948
shunt@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com