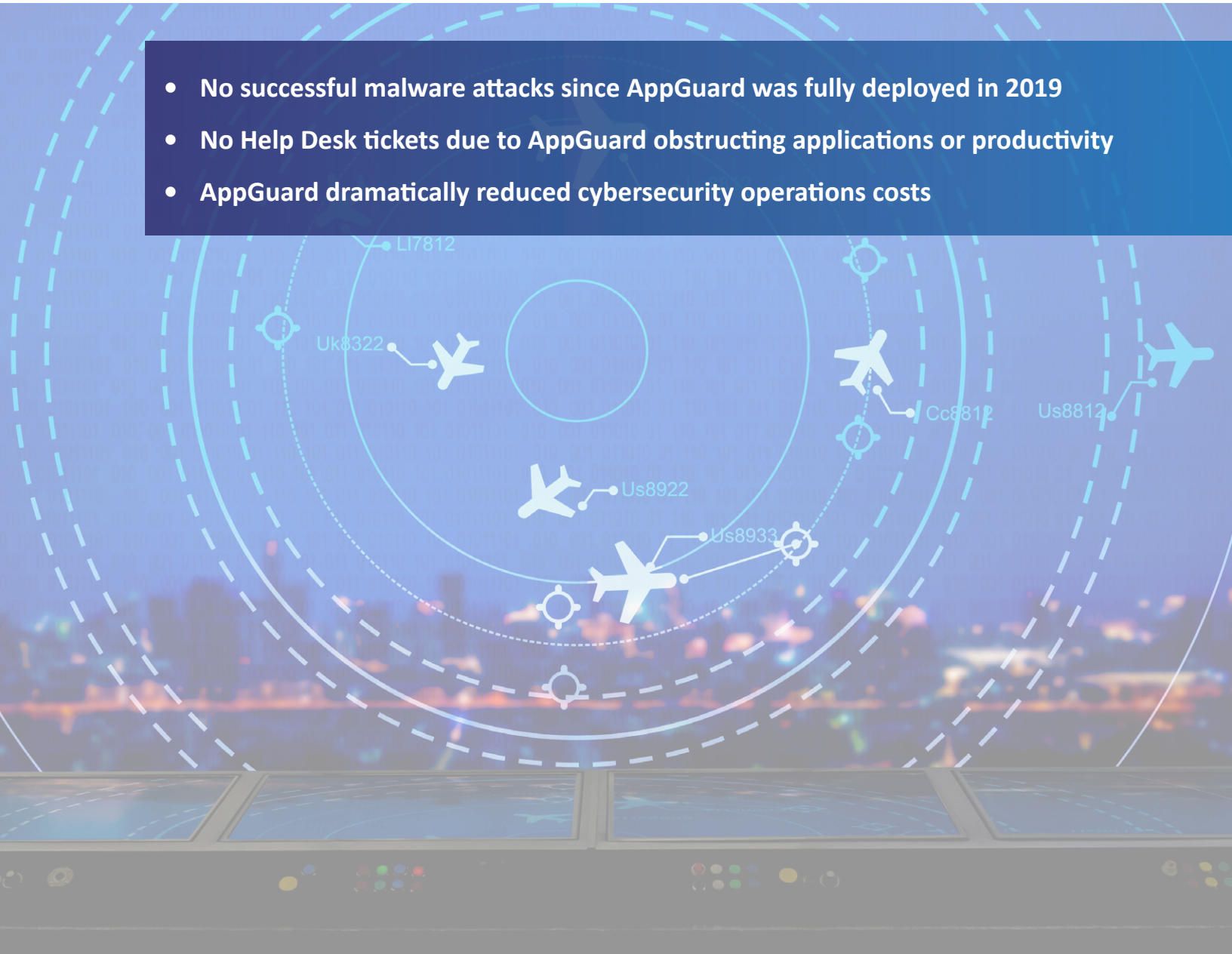
APPGUARD
Stops malware EDR/XDR miss

Case Study

All Nippon Airways (ANA): Adding AppGuard Radically Improved ANA's Cyber Defense

- No successful malware attacks since AppGuard was fully deployed in 2019
- No Help Desk tickets due to AppGuard obstructing applications or productivity
- AppGuard dramatically reduced cybersecurity operations costs



All Nippon Airlines (ANA) Case Study Summary Table

This table quickly gives readers an idea for how deploying AppGuard can benefit their organization. All quotes are from Akihiro Wada, All Nippon Airways Co., Ltd., Digital Transformation Office, General Manager, Planning & Promotion Department, Information Security and Infrastructure Strategy.

Challenges	Outcomes
Like-size organizations average over a dozen malware compromised endpoints per week	• "No successful malware attacks since AppGuard was fully deployed in 2019", including no endpoint downtime • AppGuard enforces launch, contain, and isolation controls on over 40,000 PCs and servers to stop malware attack techniques
AV and EDR fail to detect too many malware attacks	• Emotet variants hurt ANA peers for years; AppGuard protected ANA • AppGuard stopped what AV/EDR missed or detected too late
EDR requires too much labor, skills, testing, and tuning	• ANA's EDR is only used for threat hunting • Eliminated EDR alerts fatigue, testing, and tuning
Patching and remediating are onerous and late	• AppGuard containment restricts what exploited Apps can do whether zero-day or unpatched • Leaves time to test patches before deploying them
The AV/EDR way of 'Detect & react' costs too much, protects too little	• AppGuard reduced SOC/analysts hours by 66% • SOC operations went from 24 hours per day, 7 days/week to 9 hours per day, 5 days/week • Eliminated malware-caused endpoint and credential remediations
The cost of the entire cyber stack is driven by chaos in PCs and servers	• AppGuard saves "far more than $750,000 (US) per year" (minimum of $18 per PC per year) • Radically reduced attack surface by enforcing 'security by design' and zero trust policies within endpoints
Known preventative tools add too much 'friction'	• No user help desk tickets due to AppGuard since 2019 • AppGuard policies rarely require updates despite weekly application updates, patches, plug-ins, and more • Many AppGuard default policies for Microsoft, Google, Adobe, and others have not changed since 2010

Threat-specific based Protection is Inadequate

Antivirus (AV), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR) tools use various forms of pattern-matching to detect malware. They ONLY stop attacks if and when they recognize some pattern. Adversaries constantly change their malware attack patterns because they know this limitation of AV, EDR, and XDR.

In 2016, ANA was using multiple AV across its 40,000 endpoints. The effort to update AV pattern-matching data across the enterprise was onerous, particularly for locations with unreliable network availability. Too much malware was evading detection. ANA deployed an EDR in 2017, hoping to detect what AV missed. Despite EDR improvements, ANA continues to consider EDR not enough. This case study explores ANA's journey to greatly improved protection for less cost and effort.

ANA on EDR: "...took too much time to operationalize..." for too Little Gain

ANA's malware tests against multiple AV and EDR were disappointing. Their operational experience with EDR was worse. EDR detection is statistics driven. When the match is high, an attack is stopped immediately. Lower statistical confidence yields alerts or nothing. Achieving fewer false alerts and increased detection rates "require constant usability and tuning that consume my IT operations". Even so, 24 by 7 monitoring, investigation, and response capabilities were required. These demanded high-skills personnel with much experience. Work loads and work hours were long and kept personnel from their families and a work-life balance.

Ransomware presented more problems. Advanced attacks evade real-time detection. At best, the EDR generates alerts. Unfortunately, ransomware does great harm before human analysts can investigate and respond to alerts. More often than not, ransomware destroys shadow volumes so EDR roll-back capabilities fail. Now, ransomware increasingly disables and/or blinds EDR.

And finally, ANA observed significant EDR updates following malware or exploits reported in trade publications. Clever adversaries will always be ahead of threat-specific defenses. ANA concluded that a major change was necessary.

ANA Examined the Root-causes of Increasing Cybersecurity Costs and Chaos

The lifecycle costs of the typical large enterprise cyber stack are too high and threaten to grow indefinitely. Mr. Wada and his team discussed and debated the root causes.

In an enterprise, every allowed activity must be monitored, which

equates to increased IT/Sec workloads and risks. Every one to three years, the industry produces an additional cyber layer to treat unaddressed symptoms. Cyber stacks and the functional teams that operate them get more complex every year. Complex tools and practices create chaos, which demands yet more personnel. Every cyber tool, every team, every practice seems to depend on what happens within the endpoints.

They concluded that **the only way to escape the runaway costs and disappointments of the 'detect & react' cybersecurity model was to fundamentally reduce the attack surface of their endpoints**, down to the computing processes within them, as well as, the human errors of endpoint users.

"Security by Design": Part 1 of Endpoint Attack Surface Reduction

ANA redefined "security by design" for its own purposes. Most enterprises cannot control the lifecycle software development practices of the vendors that produce the 3rd party software that enterprises buy and deploy. However, ANA could control what 3rd party software runs on ANA's endpoints. ANA's "security by design" is more practical.

Every application on endpoints can potentially be hijacked to perform harmful actions that pose varied risks to the enterprise. Each application represents a potential attack surface. There were too many different applications running on different ANA laptops, desktops, and servers.

ANA's root-cause analysis led them to realize they would need to audit their endpoints, create policies for what applications are authorized. Fewer allowed applications equates to less attack surface. Creating these policies would not be easy and the addition of any new application would require a change review process.

There was skepticism among IT personnel. ANA decided to proceed in phases.

"Zero Trust WITHIN Endpoints": Part 2 of Endpoint Attack Surface Reduction

"Security by Design"

- Allowing users to install any application increases the entire enterprise attack surface
- Restrict launches and loads to what is trustworthy
- Any application or OS component can potentially be used for malicious purposes
- Many powerful OS utilities are unnecessary and pose cyber risks if allowed to run
- High-risk applications authorized to run require zero trust policies that restrict their activities
- High-value objects and applications must be isolated from the rest of the host should there be a malicious computing process despite all efforts to avoid one

Any legitimate application or OS component can potentially be used for malicious purposes, even applications with security designed into them from the start. One malicious computing process in one endpoint can substantially affect the enterprise. To this day, most zero trust frameworks do not attend to the risks within endpoints, which ANA considers the largest overall attack surface. "Security by design" reduces computing processes to authorized applications and operating system utilities. Some of these cannot be prohibited because of critical workflow dependencies.

"Zero trust WITHIN endpoints" expects that any application will at some point become malicious. Just as each application poses a potential attack surface, each application's activities pose yet more potential attack surface. Most applications don't need to spawn PowerShell, read the memory of the Windows process where credentials are stored, or write potentially malicious code into the Windows directory or registry. Fewer allowed application activities equates to less attack surface.

Policies Must be Enforced

"Zero Trust WITHIN Endpoints"

Restrict what applications can and cannot do

- Read/write/load what files/folders
- Read/write what registry keys/values
- Read/write memory of other Apps
- Allowed/prohibited child processes
- Loading of script and DLL files

(Attack Surface Reduction)

While one could uninstall all unnecessary, unauthorized applications and OS utilities with a central management system, having a kernel-level enforced tool prohibit their use would be easier, especially for OS utilities that might be reinstalled with Microsoft updates. But that only accounts for what is known to be installed. And, it eliminates sometimes valuable flexibility in letting some power users have admin rights. An Application Control tool is a better solution for allowing use of legitimate or default-denying unknown, unauthorized applications, scripts, etc.

"Security by Design" policies are supported by Application Control tools, which can restrict what applications and OS utilities can run. Some of them support parts of "Zero Trust WITHIN Endpoints", which are needed to control what running applications can and cannot do. All these reduce the endpoint attack surface, which limits what malware technique activities can succeed.

Enforcement Must be Practical

It is absolutely critical that "Security by Design" and "Zero Zrust Within Endpoints" policies must be practical to enforce. Enforcement must not inhibit authorized changes or disrupt user workflows. ANA found that known Application Control tools did not fulfill all of ANA's requirements, most still do not.

They can restrict launches but require a rule for each of an application's executables, which can be many. Worse, the rules for all of an endpoint's applications change weekly, if not daily, because of feature updates, security patches, plug-ins, etc. The administrative burden to create and maintain allow lists is far too high.

Some vendors provide allow lists for mainstream applications. However, market analysts confirm that most enterprises have so many non-mainstream applications that vendor provided allow lists relieve too little administrative burden, except for fixed-function endpoints. These run relatively few applications that change infrequently. However, ANA's ultimate goal is to reduce its overall attack surface. It sought a solution that could be practical for general purpose endpoints such as PCs and multi-purpose servers. This ruled out all tools known to ANA, and still does.

Worse, most known tools cannot enforce what running applications can and cannot do (aka, "Zero Trust WITHIN Endpoints, peri-execution, Application Containment). Those few that could, require multiple rules per application computing process. Launch control alone requires 1000s to 10,000s of rules per endpoint. Controlling what applications can do and cannot do could potentially increase the rule count up to ten times, depending on the type of endpoint and how extensively one reduces attack surface. Fewer rules equates to less administrative overhead and less disruption to user workflows.

Neither ANA nor any market analyst knew of any large scale deployments on fixed or general purpose endpoints where the activities of running applications were restricted. None of the Application Control tools known by ANA's peers could do this practically. ANA's aspirations to reimagine its overall cybersecurity posture would be academic until a viable solution would be found. Until then, ANA would have to make the best of its AV/EDR.

Why ANA Chose AppGuard

A sales presentation asserted that AppGuard could make ANA's attack surface reduction hypothesis practical. ANA immediately understood the meaning of AppGuard's name: 'guard the application'; do not allow applications to harm the endpoint, and its enterprise.

AppGuard did not apply a set of unique rules to each computing process of each and every application as other tools did (ie, an administrative quagmire). Overall, AppGuard requires hundreds of policy rules whereas tools that might theoretically match the protection assurance would require up to 100,000 rules. Further, application updates, patches, and plug-ins rarely, if ever, required policy updates for AppGuard, whereas other tools require weekly if not daily updates.

Having spent much time contemplating the fundamentals of cybersecurity and operations they **realized that AppGuard required far fewer policy rules and policy rule changes, yet AppGuard delivered far greater risk mitigation capabilities. They decided to investigate further**.

In the lab, ANA found that AppGuard coexisted with all of its other endpoint security tools. **AppGuard's memory, CPU, and disk usage was very low, less than a fifth that of Windows Defender**. Next, ANA conducted malware testing. One AV/EDR tool detected some but missed most. The other AV/EDR tools missed everything. **Unlike all of the other tools, AppGuard defeated all of the malware samples with AppGuard's default policies!**

ANA continued to investigate. They learned that AppGuard had other capabilities that could stop yet more malware technique activities not included in their testing. For example, application memory isolation and folder isolation policies prevented credential theft from Windows and cached web browser passwords, respectively. Any other tools that could do this at all were known to not do so in the field. Lastly, ANA saw they could easily customize AppGuard policies for the respective endpoints as well as adjust for future malware techniques.

In conclusion, **ANA observed that AppGuard features three fundamental controls that neutralize more malware technique activities than any other controls-based tool known, and with a fraction of the administrative overhead:**

Launch	Restrict what can launch/load	Block Malware Technique Actions within Endpoint to Stop Attacks
Containment	Protect the endpoint from the application	
Isolation	Protect parts of the host from the rest	

2018: Initial Deployment, 25,000 Endpoints

Having thought long and hard about pragmatically reducing the endpoint attack surface, ANA started AppGuard deployment with groups of fixed function endpoints, saving multi-purpose and general-purpose workstations and servers for later as their experience with AppGuard accumulated. ANA found that AppGuard aided them with refining their application inventories for their endpoints and learning what their applications do.

AppGuard's discovery mode informed ANA what legitimate activities AppGuard would have blocked so that policies could be adjusted before switching to enforcement mode. However, ANA

revised their endpoint policies, then adjusted AppGuard policies to enforce their endpoint policies.

Over time, ANA observed that application updates and security patches did not require AppGuard policy updates. **ANA confirmed that AppGuard agents really do tend to run months to years without need for policy updates**.

Any addition of a new application to an endpoint group triggered a change management process to amend ANA's endpoint policies. This included verifying that the new application would not conflict with ANA's "Security by Design" and "Zero Trust WITHIN Endpoints'' driven policies. At which time, an AppGuard policy update might be required.

At the time, this required placing AppGuard back into discovery mode. ANA wanted to minimize maintenance windows and lab testing. So, ANA helped define a 'local discovery mode' where most protections could remain in place while allowing discovery mode to run for only the new application. Local discovery mode has been serving customers ever since.

Deployments stopped at around 25,000 endpoints for different groups and locations. ANA's quest for endpoint attack surface reduction policies was well regarded, yet skepticism remained. Some IT personnel were concerned with changing their practices too fast. What if their change management can't keep up with legitimate change needs? Have they anticipated all challenges? Would help desk ticket volume increase because users cannot use authorized applications? ANA decided to pause further deployments to answer these and other questions by observing the operations with AppGuard deployed.

Incident in Early 2019, led to Full Deployment (2019)

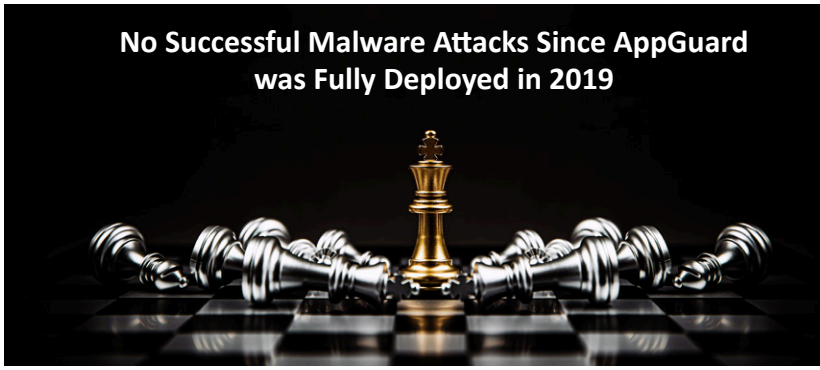
There was an "external intrusion attempt". AppGuard was the only cyber defense layer to stop it. At this point, none of the operations concerns had manifested. All of this "helped change the mindset" of those that had resisted full deployment to all 40,000 endpoints. **The value and practicality of slashing endpoint attack surface size had become widely recognized throughout ANA**.

Market analysts asked ANA how long it took them to deploy AppGuard across all 40,000: "approximately one year". This was the first time ANA and ANA's personnel had deployed such endpoint controls. "If we had to do it again, we would do it much faster."

An AppGuard certified MSSP can deploy AppGuard more quickly and more easily than most organizations because the MSSP has already done so many times for others. An MSSP deployed AppGuard on five hundred Windows Servers for a healthcare services provider over a weekend.

ANA's Experience: No Malware Compromised Endpoints Since Fully Deploying AppGuard

As of December 2023, ANA has experienced no successful malware attacks on any of its 40,000 endpoints protected by AppGuard since it was fully deployed in 2019. For 40,000 endpoints, market analysts would expect one to three dozen malware compromises per week on AVERAGE. Several market analysts were stunned when ANA told them they had suffered none since 2019. Malware endpoint compromises per week per enterprise is a statistic that is one of the most under-reported cyber statistics. Some market analysts privately say a 'half dozen per week per 5,000 endpoints' is typical. Bear in mind, some regions require disclosure or reporting of a cyber breach. And, not all malware compromises are considered a cyber breach.



How ANA Protects its Endpoints

ANA relies on Defender for AV because it is included with their Windows subscriptions from Microsoft. ANA does not use its EDR for active protection. Instead, **ANA only uses EDR for threat hunting** (ie, look for successful intrusions despite defenses). ANA is prepared to use its EDR for incident response when needed.

Before AppGuard, ANA observed how labor intensive EDR is. B**y using EDR only for threat hunting and incident response, ANA has been able to reduce its SOC analyst hours by 66%**. Employee attrition has plummeted because they can spend more quality time with their families. Normal SOC hours had been 24 x 7 x 365. Post-AppGuard, normal hours are Monday through Friday, 9 am to 6 pm.

For over four years, AppGuard has eliminated malware compromises while reducing analyst hours to a third of those needed for full-featured EDR. Better protection for less effort!

ANA's Experience: No "Friction", Easy Administration

ANA shocked market analysts with the answer to the question, how many help tickets per week on AVERAGE does ANA get from users having problems with authorized applications due to AppGuard. ANA's answer was "none". Consider this, Application Tools have been around for almost twenty years. Most enterprises removed these because they received many help desk tickets per week from end-users.

IT operations personnel would be interested to know that ANA has observed that AppGuard has rarely required a policy update because of a normal application update, patch, or plug-in. For fixed function endpoints, the time in between such AppGuard

Should All Enterprises Rely Solely on Defender and AppGuard?

Yes and no. ANA can take full advantage of AppGuard because ANA practices "Security by Design" and "Zero Trust WITHIN Endpoints"to very significantly reduce their attack surface. ANA administers AppGuard itself to customize AppGuard policies for ANA's endpoints and malware risks.

Also important, ANA employs a robust change management system to ensure that only authorized software that conforms to ANA's policies runs on its endpoints. The addition of a new application to any endpoint must undergo this process before it can be deployed. Few commercial enterprises, large or small, apply such rigor.

Remember, any allowed activity in the enterprise ought to be monitored in case it should turn out to be malicious. ANA uses its practices and its use of AppGuard to reduce allowed activities to those workflows necessary for business.

If an organization is not set up to control what applications are authorized, then defense in depth becomes more critical. For the endpoint, that would mean AppGuard plus an AV/EDR. However, many AppGuard customers have been faced with constrained resources or have cybersecurity maturity issues, they chose AppGuard over EDR because a major reduction in endpoint attack surface greatly alleviates all workloads across the cyber stack, including layers which are sometimes missing entirely.

Most AppGuard customers rely on an AppGuard certified managed security services provider (MSSP). The customer then benefits from the MSSP's experience as well as the MSSP's knowledge of malware techniques. Deployments start with default policies, tune-out any problems (usually very few), and then add more policies over time to mitigate ever more malware technique risks while accommodating necessary workflows. Also, as AppGuard is NOT a detection tool, AppGuard reports blocked actions, which may or may not be the result of a malware attack. An MSSP can analyze and report on the blocking actions as malware related, especially those that occurred months earlier before the malware detection industry learned to detect a malware attack that AppGuard had stopped months earlier.

policy updates is measured in years. For general purpose endpoints, the time measured is many months, and most of those policy updates are not due to updates, patches, or plug-ins for existing applications but for the installation of new applications.

Beyond Risk Mitigation, How Much has AppGuard Saved ANA?

Quantifying such numbers for an organization so large and for something as complex as cybersecurity is incredibly difficult. ANA's savings are "much higher than JPY100 MM ($750K) per year". At minimum, ANA has saved $18.75 per endpoint per year.

We can infer more for readers. With no malware incidents since 2019, there have been no endpoint remediations or credential resets due to malware attacks. ANA reduced its SOC analyst hours by 66%. The cost savings is likely higher because there's no higher pay for off-hours. The containment of applications with software vulnerabilities saves ANA from pulling personnel from other tasks to hurriedly implement application security patches. Considering that over half of data breaches originate at an endpoint, network security alerts have undoubtedly dropped considerably. If ANA hasn't experienced direct cost savings, ANA has certainly benefited from personnel having time to work tasks they otherwise could not. And lastly, ANA has experienced no endpoint downtime due to malware. Opportunity cost savings associated with productivity usually are higher than direct costs. Malware breaches typically cause regulatory fines and other costs. Having had no successful malware attacks since 2019, imagine those cost savings. These are additional cost savings above and beyond $18.75 per endpoint per year.