Cyber Fusion for Endpoint Security

Enhance endpoint threat detection, investigation, and response with four critical capabilities

CYWARE™

The State of Endpoint Security

Network endpoints are a popular infiltration point for attackers, as they are more exposed than an organization's crown jewels. From laptops, mobile devices, and IoT/OT infrastructure to servers and virtual environments, compromising an endpoint is a much easier proposition for an attacker than trying to gain direct access to a sensitive database or system.

So it shouldn't come as a surprise that endpoint attacks—and consequently, endpoint *security*—have become a significant pain point for security teams.

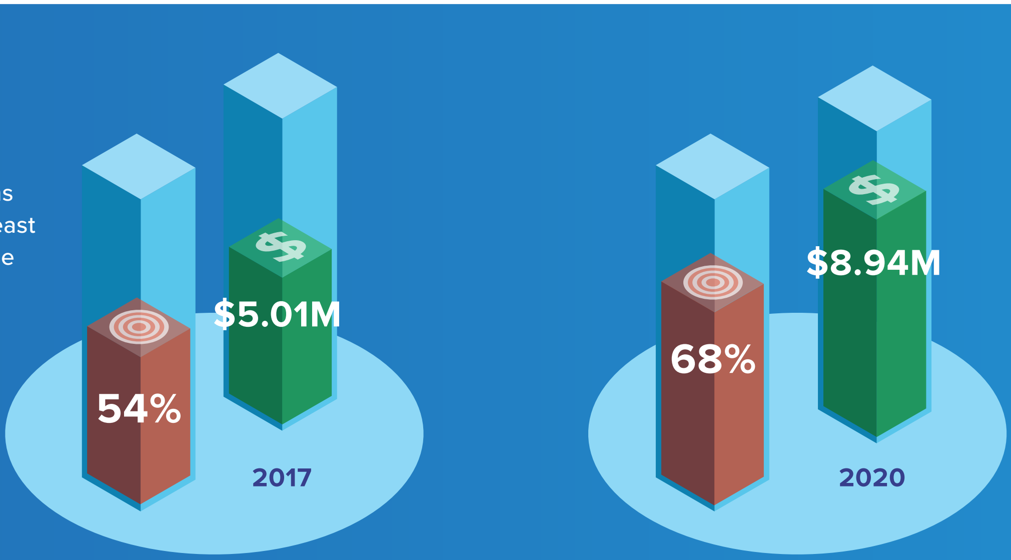
Ponemon Institute's 2020 State of Endpoint Security Risk study found that 68% of organizations "...experienced one or more endpoint attacks that successfully compromised data assets and/or IT infrastructure over the past 12 months, an increase from 54% of respondents in 2017."

In the same study, 68% of respondents said their organization's endpoints had faced a higher frequency of attacks over the preceding year. Meanwhile, the cost of successful endpoint attacks has risen from $5.01 million in 2017 to $8.94 million in 2020.

These figures paint a bleak picture. Despite a significant rise in expenditure on endpoint security tools—the market grew by 8.1% in 2020 alone and is expected to continue growing at a CAGR of 8.1% between 2021-2028—the frequency and cost of endpoint attacks are rising quickly.

Contents

Percentage of organizations that have experienced at least one endpoint attack and the cost of the attack



Source: Ponemon Institute 2020 State of Endpoint Security Risk study

What Tools are Available?

Three types of technologies dominate the endpoint security market: EDR, EPP, and XDR.

ENDPOINT DETECTION AND RESPONSE (EDR) TOOLS

These solutions record and store system-level behaviors from endpoints and use analytics to detect suspicious behavior, provide context, block malicious activity, and suggest remediation steps to protect or restore compromised endpoints.

Gartner states that EDR solutions must provide four main capabilities:

- Detect security incidents
- Contain the incident at the endpoint
- Investigate security incidents
- Provide remediation guidance

EDRs are an active security control, meaning they detect threats and aid investigation but require a human analyst to complete remediation steps.

ENDPOINT PROTECTION PLATFORMS (EPP)

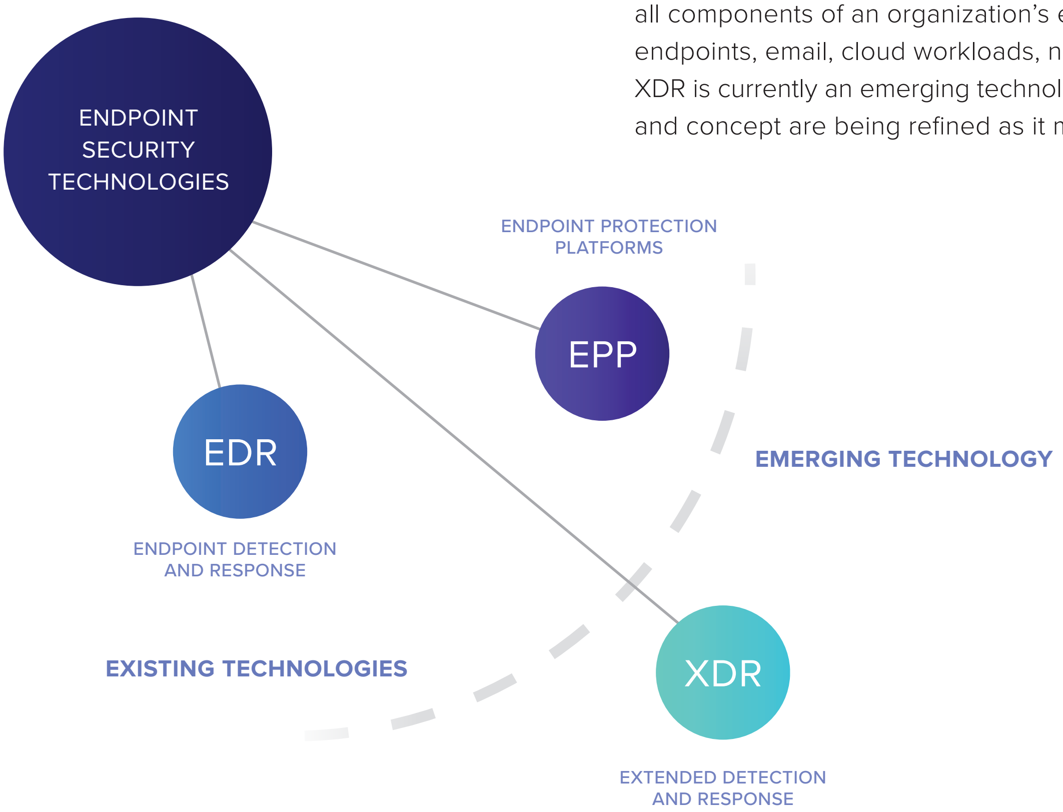
EPPs aim to prevent and protect against known and unknown endpoint threats and allow analysts to investigate and remediate incidents that evade those controls. EPP functionality includes:

- Malware signature matching
- Sandbox file testing for malicious behavior
- Behavioral analysis to identify threats with unknown signatures
- Static file analysis
- Whitelisting and blacklisting of IP addresses, URLs, and applications

Compared to EDRs, EPPs are mainly a passive control that protects against endpoint threats without requiring human supervision. However, some EPPs now incorporate EDR functionality, allowing them to perform both roles.

EXTENDED DETECTION AND RESPONSE (XDR)

XDR solutions play a similar role to EDRs, but for a broader range of assets. While EDR tools focus specifically on endpoints, XDR aims to detect and prevent threats against all components of an organization's environment, including endpoints, email, cloud workloads, networks, and more. XDR is currently an emerging technology and the definition and concept are being refined as it matures.


ENDPOINT SECURITY TECHNOLOGIES
ENDPOINT PROTECTION PLATFORMS
EPP
EDR
ENDPOINT DETECTION AND RESPONSE
EMERGING TECHNOLOGY
EXISTING TECHNOLOGIES
XDR
EXTENDED DETECTION AND RESPONSE

Several challenges stand in the way of effective endpoint security.

Endpoint Security Challenges

As it currently stands, several challenges stand in the way of effective endpoint security:

A rapidly growing number of endpoints—Digital transformation and the compulsory move to remote working have caused business networks to grow at an unprecedented rate. Gartner predicts the number of devices in use globally will rise to 6.4 billion in 2022, an increase of almost 400 million since the start of the COVID-19 pandemic—and remote work is the top cause.

Since every endpoint connected to a business network is a potential infiltration point for an attacker, this poses a substantial security threat.

Lack of visibility—The surge in endpoints intensifies a related challenge—not all endpoints are known to IT and security teams. This is partly due to so-called shadow IT, however, there's a deeper issue.

Legitimate endpoints typically have multiple agents installed on them for functions such as IPS, AV, patch management, and more. However, most organizations don't have a central repository or monitoring solution that keeps track of those agents or the endpoints they are installed on. This results in a chronic lack of visibility across the full attack surface, creating a further security risk.

Lack of human resources—The cybersecurity skills gap is well publicized, and it poses a considerable challenge for endpoint security. EDR tools do an excellent job of detecting possible issues, but they create a lot of noise in the form of false positives. With so many alerts and so few skilled analysts to process them, it's inevitable security teams will miss some genuine incidents.

Cyber Threat Intelligence (CTI) has been proposed as the solution to these challenges. However, analysts seldom have unfettered access to the intelligence they need when and where they need it. As a result, many security teams chronically underuse the CTI they collect and pay for, and continue to struggle with false positives and lack of endpoint threat context.

Complexity—With many clients installed on each endpoint and analysts using several discrete tools to identify, investigate, and resolve endpoint security issues, complexity has become a huge challenge.

At present, teams lack access to effective orchestration and automation capabilities, forcing analysts to interact manually with each tool. This is cumbersome and time-consuming, extending critical metrics such as MTTI/MTTR and putting the organization at risk. Complexity has become such a widespread issue that 50% of organizations are actively reducing the number of tools they use for endpoint security because it hinders effectiveness.

Cyber Hygiene: a Deeper Issue

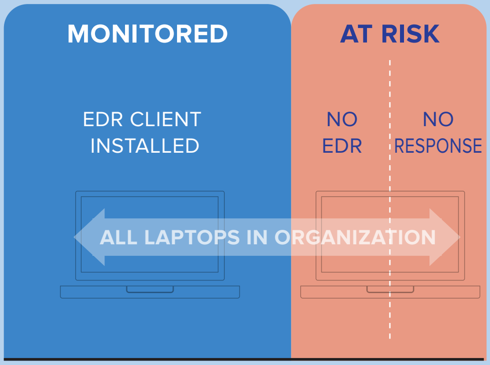
Notice how—aside from the skills gap—the challenges listed above aren't exclusively security issues. They relate to a more fundamental problem: a lack of cyber hygiene.

Without a reliable understanding of what endpoints exist, where they are, and whether they are functioning and responding correctly, effective endpoint security is impossible. There will simply be too many blindspots within the environment that hinder incident detection and response.

Why is Cyber Hygiene Important?

Imagine you have 100 laptops. Ideally, each has an EDR client installed so the security team can monitor it remotely and detect incidents. But what if that's not the case? What if 20 laptops don't have the client, and another 20 aren't responding? And what if the security team doesn't realize because they have no central system that monitors cyber hygiene? In that case, those 40 laptops become a risk because the security team won't receive EDR alerts in the event of an incident.

Effective cyber hygiene mitigates this problem by monitoring all endpoints to ensure they are properly configured, installed with all the right clients, and kept fully up-to-date.



What's Needed for Better Endpoint Security?

In its white paper Reimagining Endpoint Security, ESG explains endpoint security can no longer be treated as an isolated function. Instead, the paper notes endpoint security must: "[...] provide security teams broad protection and unified visibility into modern, sophisticated attacks."

The report goes on to explain: "[...] modern endpoint security solutions must be architected with the security operations center in mind, delivering the telemetry, visibility, investigation, and remediation capabilities required to support daily security operations."

While today's EDR and EPP tools do an excellent job of detecting incidents, they don't provide all the tools and oversight security teams need. In particular, they lack the ability to operationalize CTI to enhance the detection and response process, and the orchestration and automation capabilities needed to boost threat response outcomes while reducing manual effort. The report lays out several crucial elements required to ensure tight endpoint security, including:

- Real-time visibility of the entire endpoint environment
- Fully integrated tools that enable instantaneous data collection and response actions
- Operationalized CTI that supports incident prevention, investigation, and response without requiring manual lookups or data transfer.
- Highly configurable orchestration and automation that reduces manual work without producing false positives

Enhancing Endpoint Security with Cyber Fusion

A Cyber Fusion strategy and framework unifies all security and IT operations tools into a single solution, allowing different security functions to collaborate and share intelligence seamlessly.

A Cyber Fusion Center (CFC) solution combines the full functionality of a Security Orchestration, Automation, and Response (SOAR) and Threat Intelligence Platform (TIP) while expanding three additional essential capabilities:

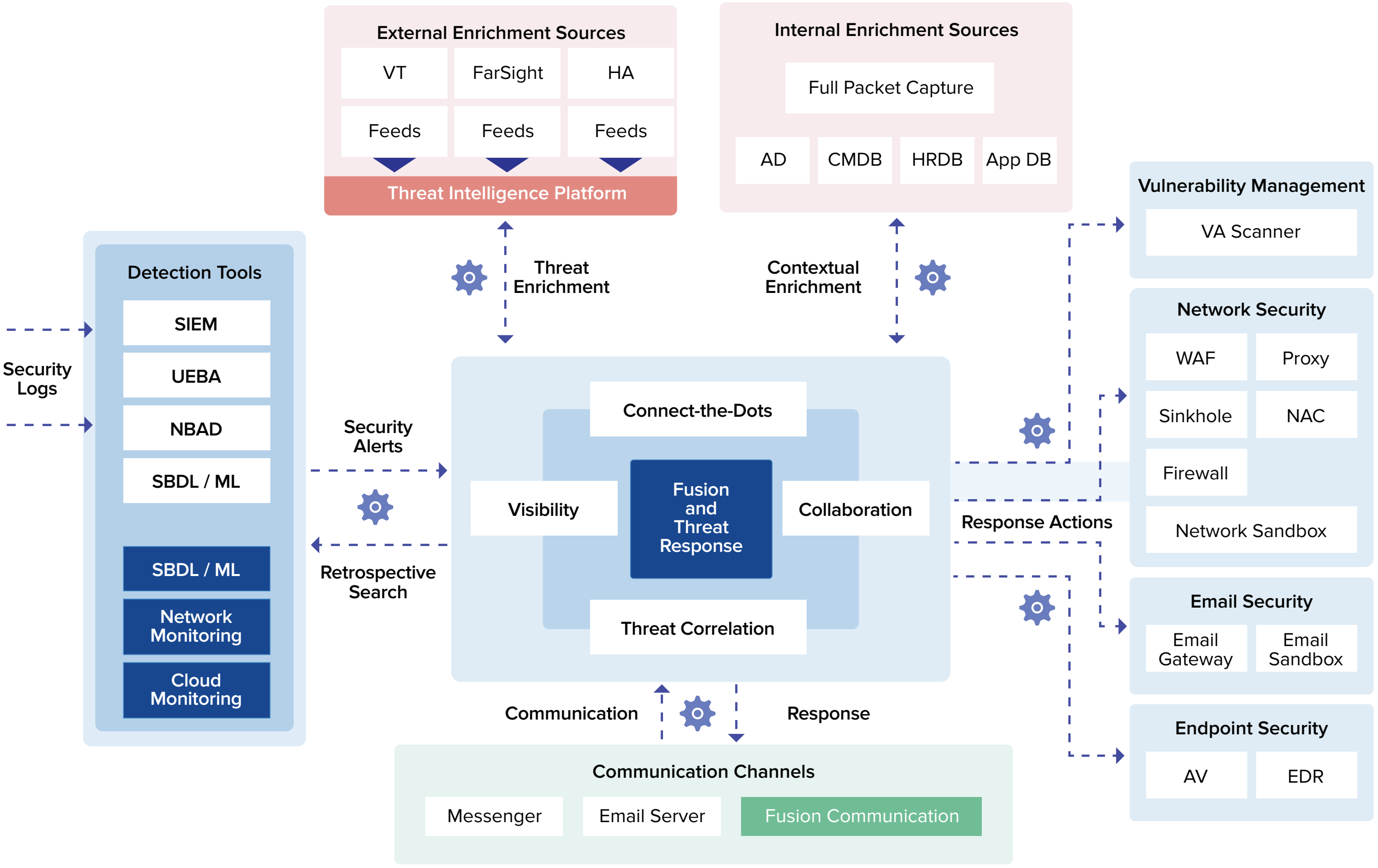
- Enhanced any-to-any integration and orchestration
- Threat intelligence sharing and collective response
- Providing situational awareness and threat context

While SOAR and TIP provide a limited version of these capabilities, it's not enough to support effective collaboration between security functions or fully empower teams to identify, investigate, and remediate endpoint threats.

Through these capabilities, CFC delivers what organizations really need to enhance endpoint security: complete visibility of their endpoint environment, instant access to all relevant CTI, and seamless orchestration and automation of hygiene, detection, and response processes.

The architecture diagram below demonstrates how a Cyber Fusion Center (CFC) solution unifies the entire security function, giving teams a single location to access all data and functionality—including that needed for endpoint security.

Cyber Fusion Center Architecture



How Does Cyber Fusion Support Endpoint Security?

A CFC solution provides four essential capabilities that support effective endpoint security:

1. **Connectivity.** A CFC solution is the connective tissue between all tools and data—not just those owned by security but also IT operations. This allows teams to maintain visibility of all endpoints no matter where they are located, ensuring they are fully operational, responsive, and up-to-date. This enforced cyber hygiene profoundly impacts endpoint security risk, as it ensures EDR and other security tools can detect threats across the entire attack surface.

2. **Any-to-any orchestration.** Many SOAR tools claim to offer comprehensive orchestration, but most are limited to integrations with specific tools or vendors. A CFC solution provides true any-to-any, cross-environment integration, and orchestration, including between internal and cloud tools. This allows security teams to seamlessly investigate and respond to threats on any endpoint without being constrained by a lack of integrations or forced to adopt specific tools.

3. **Situational awareness.** A CFC solution facilitates real-time sharing of CTI and other contextual information between security teams, roles, and organizations. This equips analysts with everything they need to investigate, triage, and respond to security incidents effectively. It also ensures security teams extract maximum value from CTI services, as insights are available to all analysts precisely when needed.

4. **Automated response.** CFC solution provides true orchestration and no-code playbook building, allowing security teams to automate time-consuming processes into a single button click. Where appropriate, playbooks can even be set to trigger automatically on set events, completely removing the burden from human analysts.

“Doesn’t SOAR do that?”

SOAR vendors position their tools as all-encompassing solutions that address many of the challenges discussed in this paper. However, most SOAR tools present several challenges:

- They provide limited integrations, often restricted to tools produced by specific vendors.
- They don’t support seamless collaboration between security teams.
- Automation capabilities often require coding skills and therefore go unused.
- They aren’t designed to support intelligence sharing between teams and organizations.

These limitations force security analysts to spend time on laborious tasks such as switching between tools, manual lookups, and data transfer.

Cyber Fusion Benefits

These capabilities provide a host of benefits for security teams, including:

- Faster MTTI/MTTR
- More consistent response
- Prioritized response to the highest-risk alerts
- Reduced manual burden on analysts
- Reduced complexity for security teams
- Fewer opportunities for human error
- Cuts out time-wasting false positive alerts
- Significantly reduced endpoint security risk

6 Cyber Fusion Use Cases for Endpoint Security

#1 Automate Endpoint Maintenance and Hygiene

One of the endpoint security challenges we explored earlier was the lack of centralized systems to ensure cyber hygiene. Cyber Fusion addresses this by combining all-to-all integration of security and IT operations tools with full machine-to-machine (M2M) orchestration, allowing security teams to build customizable playbooks that can run continuously or are triggered by specific events.

Cyber Fusion can automate critical functions such as:

- Monitoring endpoints to ensure all necessary software is present and responding.
- Installing new patches, both for security tools and other software.
- Setting up devices for new employees with the correct software and permissions.
- Automatically quarantining devices when employees leave the organization.

These measures ensure security analysts and tools have full visibility of the organization's endpoints.

#2 Contain Active Incidents Automatically or with One Click

When there's an active threat in the environment, security analysts need to work quickly. Playbooks can orchestrate complex tasks across multiple tools and endpoints in a fraction of the time, allowing analysts to quickly contain a threat once they have identified it. For example, if several endpoints are infected with malware, an analyst could use a playbook to quarantine them all with one click.

Cyber Fusion also allows security teams to set playbooks to run automatically when specified events occur. For example, if an endpoint becomes infected with ransomware, a playbook could automatically quarantine that device from the rest of the network.

#3 Endpoint-appropriate Response

Of course, taking automated action against an endpoint could be a risk. Automatically quarantining a non-critical endpoint—for example, a laptop infected with ransomware—is usually a good option. But what if the endpoint is more important?

Cyber Fusion allows security teams to set automated responses based on the criticality of the endpoint affected. For example, an infected laptop can be quarantined, but an infected cloud server requires an urgent alert to the asset owner and other stakeholders.

#4 Incident Enrichment and Categorization

One of the top challenges security analysts face is constantly switching between tools. This is particularly noticeable when an analyst is gathering context to determine how to act on an alert. Typically, this process involves manually switching between tools, searching for relevant intelligence, and copying any information they find back into their case management tool.

Many tool vendors claim to solve this problem, but they invariably rely on 1-1 integration. This reduces some of the analyst's burden, but they still have to do a lot of manual work. Cyber Fusion provides all-to-all integration and orchestration, allowing analysts to enrich cases with all relevant intelligence and data no matter where it resides. This drastically reduces the manual burden of incident enrichment and will enable analysts to categorize and prioritize incidents easily.

A Cyber Fusion Center solution also tracks incidents over time and provides valuable context within the case management system. For example, if a new incident is similar to a previous one, the solution will automatically link them so the analyst can see how the last incident was handled.

Cyber Fusion provides access to shared intelligence vetted by people in your vertical, one of the most valuable security assets. We operationalize intelligence in several ways, including to support our endpoint security. Intelligence sharing, orchestration, and automation using Cyber Fusion is how organizations can improve detection and prevention, particularly for advanced and future threats.

Ahmed Pasha

EXECUTIVE DIRECTOR AT
GLOBAL FINANCIAL SERVICES
GROUP NOMURA

#5 Up-tier Analysts by Automating Manual Tasks

Tier 1 analyst tasks like host attribution, tagging, and incident categorization consume a lot of time. This harms security outcomes, and it's also frustrating and demoralizing for security analysts to spend so much of their time on manual, repetitive tasks.

With a combination of all-to-all integration, orchestration, and automation, Cyber Fusion can automate most Tier 1 activities, allowing analysts to spend more time on Tier 2 and 3 activities that significantly impact cyber risk.

#6 Remote Forensics

Investigating complex security incidents requires analysts to gather as much information as possible. Typically, this involves manually accessing affected endpoints and using the command line to find, collect, and send relevant logs back to the analyst's machine.

A Cyber Fusion Center solution can integrate directly with EDR tools to issue remote commands to any endpoint. Playbooks can automate the process of remotely gathering forensic information like connection data, logs, and memory imaging into a single JSON object and sending it to the analyst.

This fully equips the analyst to investigate the incident while removing the manual burden.

Crush Endpoint Threats with Cyber Fusion

Despite a surge in spending, most enterprises are experiencing worse endpoint security outcomes with each passing year. While current tools are good at identifying possible incidents, they don't provide the broader functionality needed to protect against the growing onslaught of sophisticated endpoint threats.

This paper has made a case for Cyber Fusion as a way to orchestrate a comprehensive response to endpoint threats while reducing the manual burden on security teams.

Key learning points include:

- **Endpoint security has become a pressing issue for security teams that isn't fully addressed by current EDR, EPP, and XDR solutions.**
- **In addition to established security challenges like the skills gap, lack of visibility, and basic cyber hygiene is among the top barriers to effective endpoint security.**
- **The top requirements for faster and more effective endpoint security are improved visibility, cross-environment integration, greater use of CTI, and configurable automation.**
- **Cyber Fusion unifies security and IT operations tools into a single solution, allowing security teams to more effectively identify, investigate, and respond to endpoint security threats.**
- **Cyber Fusion solutions support better endpoint security outcomes by delivering all four of the additional requirements described in this paper.**
- **The top benefits of Cyber Fusion for endpoint security include faster MTTI/MTTR, decreased complexity and manual burden for security teams, and significantly reduced cyber risk.**

This paper has laid out six common use cases for Cyber Fusion in endpoint security. In practice, there are many more applications to reduce cyber risk and the manual burden on security teams.

To see how Cyware's virtual Cyber Fusion Center solution can help your enterprise security team boost collaboration and improve endpoint threat response, arrange a free demo today.

About Cyware

Cyware helps enterprise cybersecurity teams build platform-agnostic virtual cyber fusion centers. Cyware is transforming security operations by delivering the cybersecurity industry's only ***virtual*** cyber fusion center platform with next-generation SOAR (security orchestration, automation, and response) technology. As a result, organizations can increase speed and accuracy while reducing costs and analyst burnout. Cyware's Virtual Cyber Fusion solutions make secure collaboration, information sharing, and enhanced threat visibility a reality for enterprises, sharing communities (ISAC/ISAO), MSSPs, and government agencies of all sizes and needs.

CYWARE™

228 Park Avenue S #77147
New York, NY 10003-1502
855-MY-CYWARE • sales@cyware.com

www.cyware.com