PLENUM TECHNOLOGIES

The Tech Tide: Zero Trust Threat Detection And Response, Q2 2021

TECH TIDE REPORT

Seventeen Technologies Underpin Zero Trust Detection And Response

Summary

Zero Trust threat detection and response is increasingly critical to firms' ability to win, serve, and retain customers. To accelerate their performance in threat detection and response, companies are evaluating and adopting a range of contributing technologies. This Tech Tide report presents an analysis of the maturity and business value of the 17 technology categories that support Zero Trust threat detection and response. Security and risk professionals should read this report to shape their firm's investment approach to these technologies.

Leverage Detection And Response For Swift, Informed Action

As attacks increase in sophistication and destruction, corporate boards and management teams no longer ask, "How secure are we?" but, "How ready are we to respond?" Detection and response capabilities have become even more critical for identifying ongoing attacks that may have evaded preventive controls and tools.

Curate A Set Of Technologies That Enable Zero Trust Threat Detection And Response

This report interviewed technology decision-makers, suppliers, and other subject matter experts in our search for the most important Zero Trust (ZT) detection and response technologies. Each of the technology categories analyzed in this Tech Tide meets three criteria and:

- **Is an important contributor to a successful Zero Trust strategy.** Data protection is the core mission of the Zero Trust model. The technologies highlighted in this report enable you to detect and respond to attacks that seek to exfiltrate or undermine your firm's most valuable data — from the personal information of customers and employees to intellectual property.

- **Is applicable to a wide range of organizations.** This report included only technologies that can protect organizations of various sizes, industries, and regions and that can scale to even the largest companies with global footprints.

- **Is a frequent source of inquiry by clients.** Technologies in this report are in various states of market maturity, from emergent to long established but declining. We offer our analysis of their current state of Zero Trust threat detection and response to help you track emerging markets and avoid investing in technologies with limited or decreasing potential. We also offer insight into where technologies are merging, are being subsumed by others, or require higher process maturity to gain full benefit.

Select Detection And Response Technologies That Offer High Business Value

The central 2x2 graphic offers a summary of the state of the technology categories that make up ZT threat detection and response (see Figure 1).

Figure 1

Tech Tide: Zero Trust Threat Detection And Response, Q2 2021

TECH TIDE

Zero Trust Threat Detection And Response

Q2 2021

Evaluate Business Value And Maturity For Each ZT Threat Detection And Response Technology

We plot the categories on two dimensions:

- **Business value.** This report evaluated the business value of each ZT threat detection and response technology on its contribution to the business in three directions: 1) how successful the technology will be over its lifetime; 2) how broad the detection and response use case is for each technology; and 3) ability for security pros to increasingly detect and remediate attacks without the burden of increasing staff.

- **Maturity.** We derived each ZT threat detection and response technology's maturity level by vetting vendor inputs and report estimates regarding the speed at which the technology will mature, vendors' current product revenue and estimated global market, and our own knowledge of the technology.

Determine ZT Threat Detection And Response Based On Business Value And Maturity

The business value and maturity dimensions, in turn, position each category in one of four quadrants:

- **Experiment.** Low maturity and low business value characterize technologies in the Experiment zone. Most enterprises should limit their exposure to these technologies to bounded experiments, waiting for the expected business value of these newer categories to improve before investing.

- **Invest.** Low maturity and high business value characterize technologies in the Invest zone. These new technologies have ripened to the point where enterprises can confidently invest.

- **Maintain.** High maturity and high business value characterize technologies in the Maintain zone. These are the bread-and-butter technologies that most enterprises rely on to run their business. They're generally stable, well-understood technologies that continue to have high returns to the business. Most enterprises should maintain their installations and usage of these technologies.

- **Divest.** High maturity and low business value characterize technologies in the Divest zone. These older technology categories have reached a point where their business

value has dropped. Most enterprises should be looking for newer, higher-value replacements and divesting from these categories.

Invest In And Maintain ZT Technologies With High Business Value

When preventive technologies are undermined, quick detection and response is the only thing standing between you and a costly, likely very public data breach. The longer an attacker has unfettered access to systems, the more damage they can cause. Threats like ransomware can spread across networks in minutes if not quickly detected and stopped. Over the past several years, emphasis has shifted from network security to endpoint and cloud monitoring technologies as the network continues to evolve. In mapping the futures of the detection and response technologies in the Zero Trust ecosystem, we found that:

- **Choice abounds in this space.** From EDR, MDR, XDR, and MSSP to CWA, SA, and SOAR, a veritable acronym soup of security solutions and services stand at the ready to take unwanted or, often, commoditized tasks and processes off your team's plate. But the purchasing decision brings its own complexities, especially when factoring in organization size, industry, geography, and internal priorities and capabilities. When selecting a detection and response solution, carefully think about how this solution will augment, rather than replace, the human elements of your SOC and enhance the skills and capabilities of your team.

- **Once-vital standalone solutions are now features.** Tools like automated malware analysis (sandboxing), data loss prevention (DLP), and security user behaviour analytics (SUBA), once considered backbones of malware detection, data protection, and insider threat programs, are now relegated to required capabilities in more-comprehensive detection and response solutions. As pressure to consolidate tech investments mounts, security leaders must consider divesting standalone solutions unless they meet a specific or critical program need.

- **Nailing the dress rehearsal is critical to comprehensive incident response (IR).** As company-crippling ransomware and novel, more-sophisticated attacks continue to rise, it's critical to have more than an IR plan and a forensics retainer in place. You must train, coach, and rehearse that plan with the security team,

executives, and other stakeholders before a real-life incident occurs. IR services often include time for executive tabletop exercises — take advantage of it. And test the power of cyber ranges to bring home the reality of an attack to executives with a fully immersive breach simulation experience.

Experiment With Cyber Range Services And Others

Three of the 17 technologies fall into the Experiment quadrant of the Tech Tide, with low (or stalled, in the case of in-person cyber range experiences) maturity and low current business value. Each of these technology categories has the potential to mature and reach higher levels of business value and adoption, although some will likely be subsumed into other solutions.

Cyber Range Services

Cyber ranges aren't just about training security incident response analysts; they're a full immersion experience for cross-functional teams of business, IT, and security professionals using real-world scenarios that mimic the genuine stress and havoc of a cybersecurity incident. Cyber ranges don't just help cross-functional teams learn good cybersecurity best practices for incident response; they help teams train under pressure. They also help teams evaluate the latest cybersecurity techniques and can be used as command centres during incidents (see Figure 2).

Figure 2

Experiment: Cyber Range Services

Strategy:
EXPERIMENT

MATURITY
Low

BUSINESS VALUE
Low

LIFECYCLE COST
$$$

SAMPLE VENDORS
Accenture; Booz Allen Hamilton; Cyberit; Deloitte; IBM; KPMG; Palo Alto Networks; Raytheon

Cyber range services

Definition
Cyber range services are physical and virtual training facilities that simulate large-scale cyberattacks. These services are used to help security teams and counterparts in IT and the business train on their cyberresponse plan to ensure a cohesive response in the event of an incident.

Maturity rationale
This emerging space was, for physical ranges specifically, set back in 2020. However, the growing demand for real-world breach training has seen a few key players making continued investments in virtual platforms.

Business value rationale
Cyber range services help cross-functional teams learn best practices of good cybersecurity incident response under pressure. Given the inevitability of a breach and the staffing and skills gap in the security industry, most security teams find value in these services and regular exercises.

Deception Technology

Deception technology detects attackers who have already infiltrated your network by mimicking high-value production applications and systems to lure attackers into interaction that will uncover their presence. This report recommends investing in capabilities that help detect and respond to threats on your actual endpoints, before experimenting with deception technologies (see Figure 3). Deception technology makes the most sense for advanced security teams who have already invested in and matured core prevention and detection tech and in high-security environments or industries that suffer frequent attacks.

Figure 3

Experiment: Deception Technology

Strategy:
EXPERIMENT

MATURITY
Low

BUSINESS VALUE
Low

LIFECYCLE COST
$$$

SAMPLE VENDORS
Acalvio; Attivo Networks; Cymmetria; Illusive; Minerva Labs; TrapX

Deception technology

Definition
Deception technologies create false IT assets to act as honeypots for cybercriminals and malicious insiders. Interaction with these false assets generates an alert. These alerts have high fidelity, as any interaction with such an asset is a business use case violation.

Maturity rationale
Solutions show improved scale, ease of deployment, and reduction of false positives. Today's vendors are adding additional features to help turn this niche into a full product offering.

Business value rationale
Deception tech may help detect cybercriminals and malicious insider activity, but it won't make your network more resilient to attack. For the average enterprise security team, it's not a top investment priority, but it can augment the toolset of more mature teams and environments.

Extended Detection And Response

Security teams struggle to address threats confidently and quickly in their environment. Extended detection and response (XDR) tools provide behavioral detections across security tooling to deliver high-efficacy alerts, additional context within alerts, and the ability to detect, investigate, and respond from a single platform. Most current XDR platforms are limited in scope for visibility, detection, and response to endpoints, offering integrations with other tools like NAV and log data collection. While limited currently, this scope is expected to expand in the future (see Figure 4).

Figure 4

Experiment: Extended Detection And Response

Strategy:
EXPERIMENT

MATURITY
Low

BUSINESS VALUE
Low

LIFECYCLE COST
$$$

SAMPLE VENDORS
McAfee; Microsoft; Palo Alto Networks; SentinelOne; Trend Micro

Extended detection and response

Definition
Extended detection and response (XDR) brings behavioral detection and response capabilities from the endpoint to network analysis and visibility tools and security log data analysis. XDR stems from a foundation of endpoint detection and response (EDR) capabilities, extended to other tooling in the SOC for unified visibility, detection, and response.

Maturity rationale
While XDR is still nascent, understanding how these detection and response capabilities can extend beyond the endpoint to unify other tools in the SOC will position security pros for long-term success.

Business value rationale
Security teams struggle with visibility, lack of context, and high false positives. XDR unifies an array of tooling to give analysts fewer false positives, additional context, and the behavioral detection and response capabilities developed for EDR solutions.

Invest In Cloud Workload Security And Others

Five of the 17 ZT technologies fall into the Invest quadrant of the Tech Tide, with low maturity and high current business value. When evaluating technologies in this category, keep in mind that they should offer value today by innovating threat detection and response. However, make sure these solutions remain in line or ahead of your own maturity with aggressive roadmaps and solid, transparent feedback loops to increase usability and/or broader applicability.

Cloud Workload Security

Cloud adoption is widespread, and it demands that security pros use cloud workload security (CWS) technologies to secure workload execution in IaaS and PaaS environments. These workloads present great security challenges due to their release speed, increasing number, and ephemeral nature. As a result, they require specialized CWS technologies to properly control and monitor them. Because CWS technologies are cloud-based themselves, security pros should expect mainly cloud-based policy servers and pricing (see Figure 5).

Figure 5

Invest: Cloud Workload Security

Strategy:
INVEST

MATURITY
Low

BUSINESS VALUE
High

LIFECYCLE COST
**$$**$

SAMPLE VENDORS
AWS; Bitdefender; Broadcom; Check Point Software Technologies; Cisco; CrowdStrike; GCP; McAfee; Microsoft; Palo Alto Networks; Qualys; Trend Micro

Cloud workload security

Definition
Cloud workload security (CWS) solutions offer visibility and protection for all components of the hybrid cloud workload stack.

Maturity rationale
CWS solutions still have gaps to cover the entire spectrum of needed functionality. Large vendors are making strategic acquisitions to fill those gaps and provide end-to-end, complete CWS suites, which increasingly include cloud security posture management (CSPM) and cloud identity governance (CIG).

Business value rationale
CWS ensures governance, visibility, vulnerability, and control of all workloads and configurations. Enterprises must have processes for automated creation and configuration of workloads for agent- and API-based operations.

Endpoint Detection And Response

Endpoint detection and response (EDR) solutions are the next generation of endpoint protection, providing more visibility and control than has ever been available. These capabilities add so much value to organizations that EDR is quickly becoming the central agent running on the endpoint that provides data for delivering features such as file integrity monitoring, vulnerability management, and the antimalware component of traditional endpoint protection (see Figure 6).

Figure 6

Invest: Endpoint Detection And Response

Strategy:
INVEST

MATURITY
Low

BUSINESS VALUE
High

LIFECYCLE COST
**$$**$

SAMPLE VENDORS
BlackBerry; Broadcom (Symantec); Cisco; CrowdStrike; Cybereason; Digital Guardian; Elastic Security (Endgame); ESET; FireEye; RSA; SentinelOne; VMware (Carbon Black)

Endpoint detection and response

Definition
Endpoint detection and response (EDR) enables high-fidelity detection behavioral analysis and precise response actions through the collection and monitoring of security-relevant operations for symptoms of misuse. This telemetry data is exposed to the security operations team through a threat-hunting interface to enable investigating.

Maturity rationale
EDR has become a best practice, with security teams that now commonly deploy the technology across both their endpoint and server environments.

Business value rationale
This market has clear segmentation, with some vendors focused on threat hunting and others automating remediation to fulfill the traditional endpoint protection value proposition of organizational resilience. When selecting a vendor, consider your threat model and security maturity.

Managed Detection And Response

Managed detection and response (MDR) services offer assurance that your business is not currently compromised via threat hunting, granting access to experts to perform investigations, and working with seasoned incident response pros to choose the best possible response action given the situation (see Figure 7).

Figure 7

Invest: Managed Detection And Response

Strategy:
INVEST

MATURITY
Low

BUSINESS VALUE
High

LIFECYCLE COST
**$$**$

SAMPLE VENDORS
Arctic Wolf; Binary Defense; CrowdStrike; Expel; Rapid7; Red Canary; Secureworks; SentinelOne; Trustwave

Managed detection and response

Definition
Managed detection and response (MDR) is the application of advanced analytical techniques, proactive threat hunting, and automated response based on escalation workflows predefined by an MSSP. The capabilities and quality of services depends on endpoint detection and response software, network analysis and visibility tools, and security log data analysis.

Maturity rationale
Since MDR came to market, the number of service providers touting the capability has grown substantially. With more companies entering the market, consolidation is guaranteed.

Business value rationale
Working with an MDR service is a philosophical change for clients accustomed to working with traditional MSS firms. These services assure your business is not currently compromised, complete investigations in hours, and provide on-demand access to IR experts.

Security Analytics Platforms

It's critical for security leaders to quickly detect and respond to cyberthreats. Infrastructure complexity, increasing data volumes, and rapidly evolving threats overwhelmed legacy rules-based SIEM solutions and forced vendors to expand them into security analytics (SA) platforms. SA platforms combine big data infrastructure, SUBA, and network analysis and visibility (NAV) with traditional SIEM capabilities. Some integrate SOAR for orchestrated processes and automation to give S&R pros better visibility, improved detection, and enhanced workflow (see Figure 8).

Figure 8

Invest: Security Analytics Platforms

Strategy:
INVEST

MATURITY
Low

BUSINESS VALUE
High

LIFECYCLE COST
$$$

SAMPLE VENDORS
AT&T; Exabeam; FireEye; Fortinet; Gurucul; Huntsman Security; IBM; LogRhythm; McAfee; Micro Focus; Rapid7; RSA; Securonix; Splunk

Security analytics platforms

Definition
Security analytics (SA) platforms are built on big data infrastructure, combining logging, correlating, and reporting feeds from security information and event management (SIEM), security solutions, network flow data, threat intelligence, endpoints, cloud environments, and applications. It uses this information and machine learning techniques for real-time monitoring and analytics. Many facilitate analysis, investigation, and response.

Maturity rationale
Many enterprises are still using legacy SIEM solutions and haven't upgraded their approach. Legacy SIEM vendors have evolved their solutions into SA platforms in the past few years.

Business value rationale
Security teams typically deploy SA platforms as the core technology in their SOC, aggregating security data and events, much as a SIEM did, while adding an analytics layer along with automation.

Security Orchestration, Automation, And Response (SOAR)

Security teams are under constant stress to quickly detect and respond to threats. Previously referred to as security automation and orchestration (SAO), SOAR tools make security teams more efficient by orchestrating processes and automating response actions, removing much of the manual work currently performed by security analysts. They act as security middleware, facilitating communication and action between security solutions that previously did not talk to each other. Most current SOAR implementations focus on expediting threat triage and investigation but also enable automated response to limit the impact of cyberattacks (see Figure 9).

Figure 9

Invest: Security Orchestration, Automation, And Response

Strategy:
INVEST

MATURITY
Low

BUSINESS VALUE
High

LIFECYCLE COST
**$$**$

SAMPLE VENDORS
Exabeam; FireEye; Fortinet; IBM; Palo Alto Networks; Proofpoint; Rapid7; ServiceNow; Siemplify; Splunk; Swimlane; ThreatConnect

Security orchestration, automation, and response

Definition
Security orchestration, automation, and response (SOAR) solutions are technology products that provide automated, coordinated, and policy-based action of security processes across multiple technologies, making security operations faster, less error-prone, and more efficient.

Maturity rationale
SOAR has only been around for a few years, with many security pros reluctant to deploy the technology due to initial concerns about automating security tasks. Adoption has accelerated, but the technology is not yet mainstream. SOAR is increasingly delivered as part of an SA platform and not a standalone.

Business value rationale
Security teams struggle with staffing, threat detection, and speed of response. SOAR tools orchestrate security processes, automate response actions, and inform analysts, allowing security teams to operate more efficiently and effectively.

Maintain Cybersecurity Incident Response Services And Others

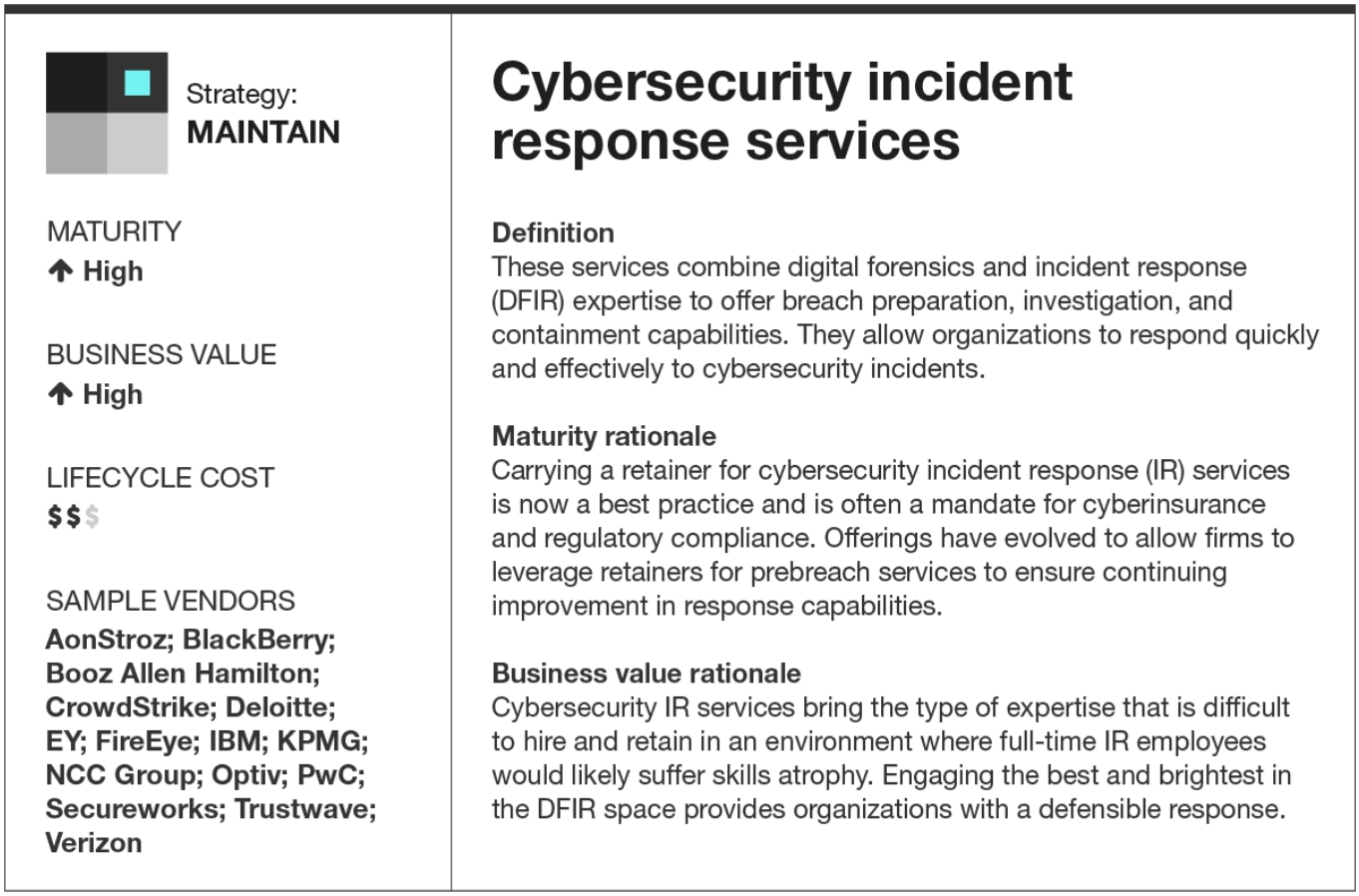
Four of the 17 technologies fall into the Maintain quadrant of the Tech Tide, with high maturity and high current business value. When evaluating technologies in this category, keep in mind that while they offer value today, there may be capabilities in the Invest or Experiment quadrants which will replace them. Keep an eye on roadmaps and acquisitions, provide feedback to your key tech providers, and be prepared to make a switch if there is a clear detection or response gap.

Cybersecurity Incident Response Services

Cybersecurity incident response services include prebreach planning and assessment services such as playbook reviews and tabletop exercises in addition to incident response and investigation/forensics in the event of a security incident. These services usually come through a retainer, creating a partnership that lets the service provider tune staffing and services for continual improvement (see Figure 10).

Figure 10

Maintain: Cybersecurity Incident Response Services



Enterprise Fraud Management

The enterprise fraud management (EFM) market is growing, as more security, fraud, and other risk professionals see EFM solutions as a way to address their top fraud management challenges and how these challenges impact customer acquisition and retention. As legacy, rule-based EFM risk scoring becomes outdated and less effective, improved, out-of-the-box AI and machine learning support for more transaction types and better data integration will dictate which providers will lead the pack. Vendors that can provide this, as well as dashboards and options for cloud and on-premises EFM deployment models, position themselves to succeed (see Figure 11).

Figure 11

Maintain: Enterprise Fraud Management

Strategy:
MAINTAIN

MATURITY
↑ High

BUSINESS VALUE
↑ High

LIFECYCLE COST
$$$

SAMPLE VENDORS
BAE Systems; Featurespace; FICO; Guardian Analytics; IBM; NICE Actimize; SAS

Enterprise fraud management

Definition
Enterprise fraud management (EFM) solutions screen transactions across users, accounts, processes, and channels to identify and prevent fraud in an organization.

Maturity rationale
Financial services institutions must increase customer acquisition and retention rates. In doing so, they also must stay within industry benchmarks for fraud loss rates and investigation labor cost. Fraud loss rates are three to 10 basis points for card fraud and less than 10 basis points for noncard fraud.

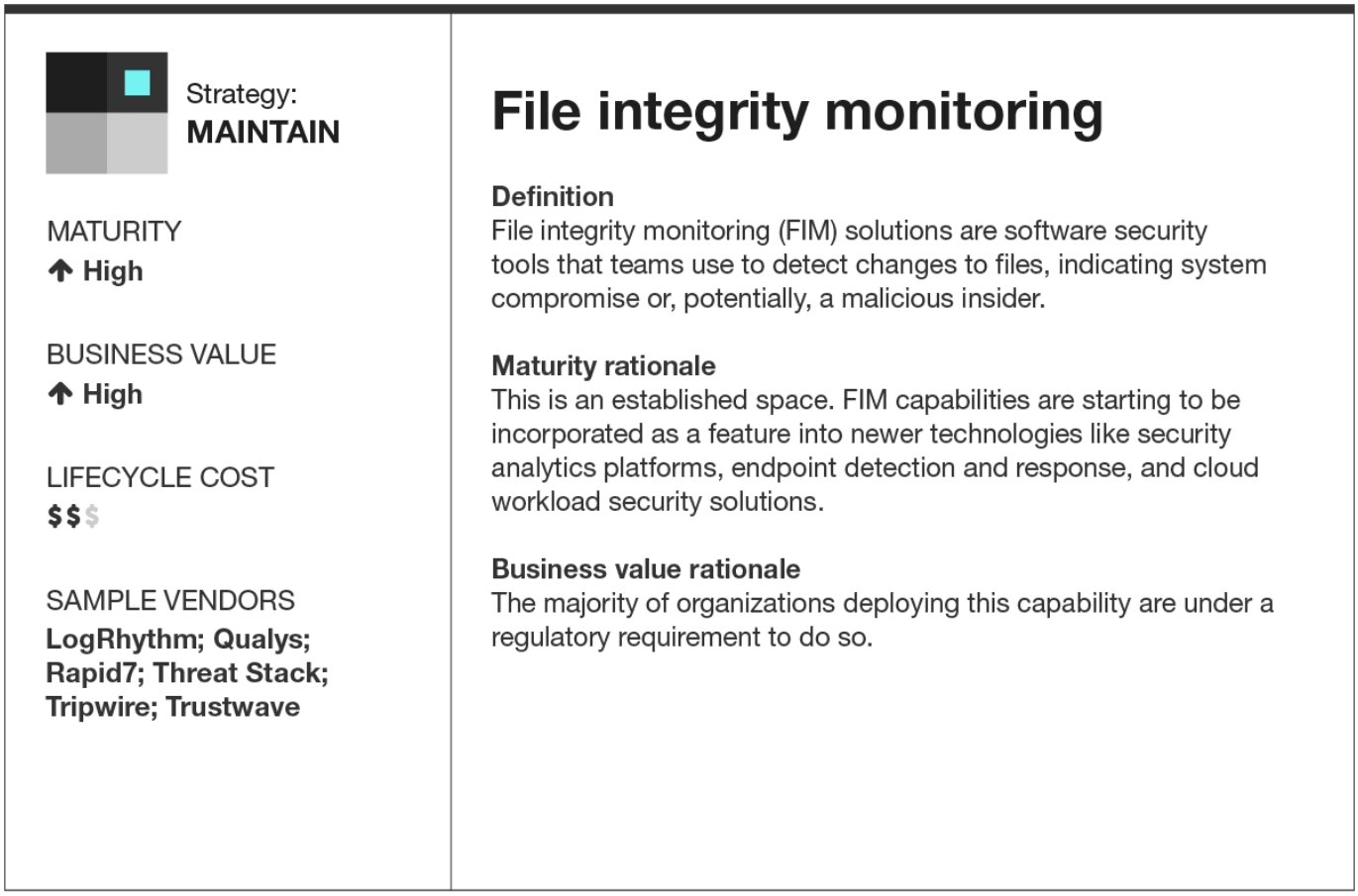
Business value rationale
These tools are incredibly important to fraud, security, and other risk pros in that they consistently balance investigative labor costs while improving the customer experience by reducing false positive rates.

File Integrity Monitoring

File integrity monitoring (FIM) is a mature technology; initially focused on guaranteeing that executables hadn't been tampered with in an attempt to backdoor a system, the use cases have evolved to detecting modification of any critical files. The majority of organizations deploying FIM do so because of regulatory requirements such as FISMA, HIPAA, PCI DSS as well as standards like NIST and the CIS security benchmarks. Many cloud workload security tools have file integrity monitoring capabilities today. Long term, more EDR solutions will also offer similar functionality, which will call into question the long-term viability of FIM as a standalone offering (see Figure 12).

Figure 12

Maintain: File Integrity Monitoring

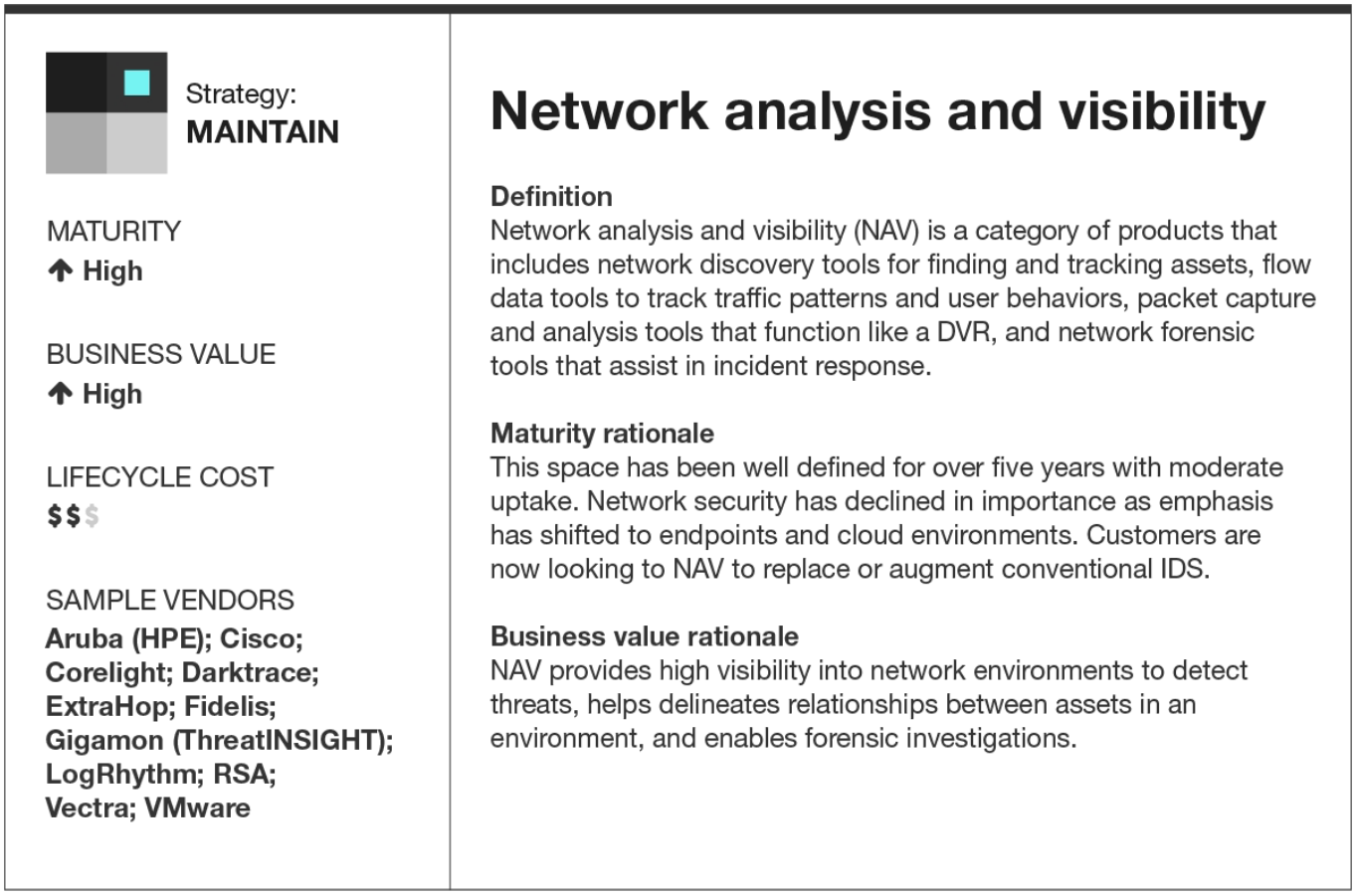


Network Analysis And Visibility

Network analysis and visibility (NAV) tools provide situational awareness and visibility for networking and security pros. NAV tools continuously scan the network for malicious activity, user and device behaviours, and potential attacks. They can search deep inside network packets and internal cloud traffic to inspect traffic flows, looking for potential attacks or malicious insider abuse. Some vendors use AI, machine learning, and behavioural anomaly detection to identify malicious behaviours (see Figure 13).

Figure 13

Maintain: Network Analysis And Visibility



Divest From Automated Malware And Others

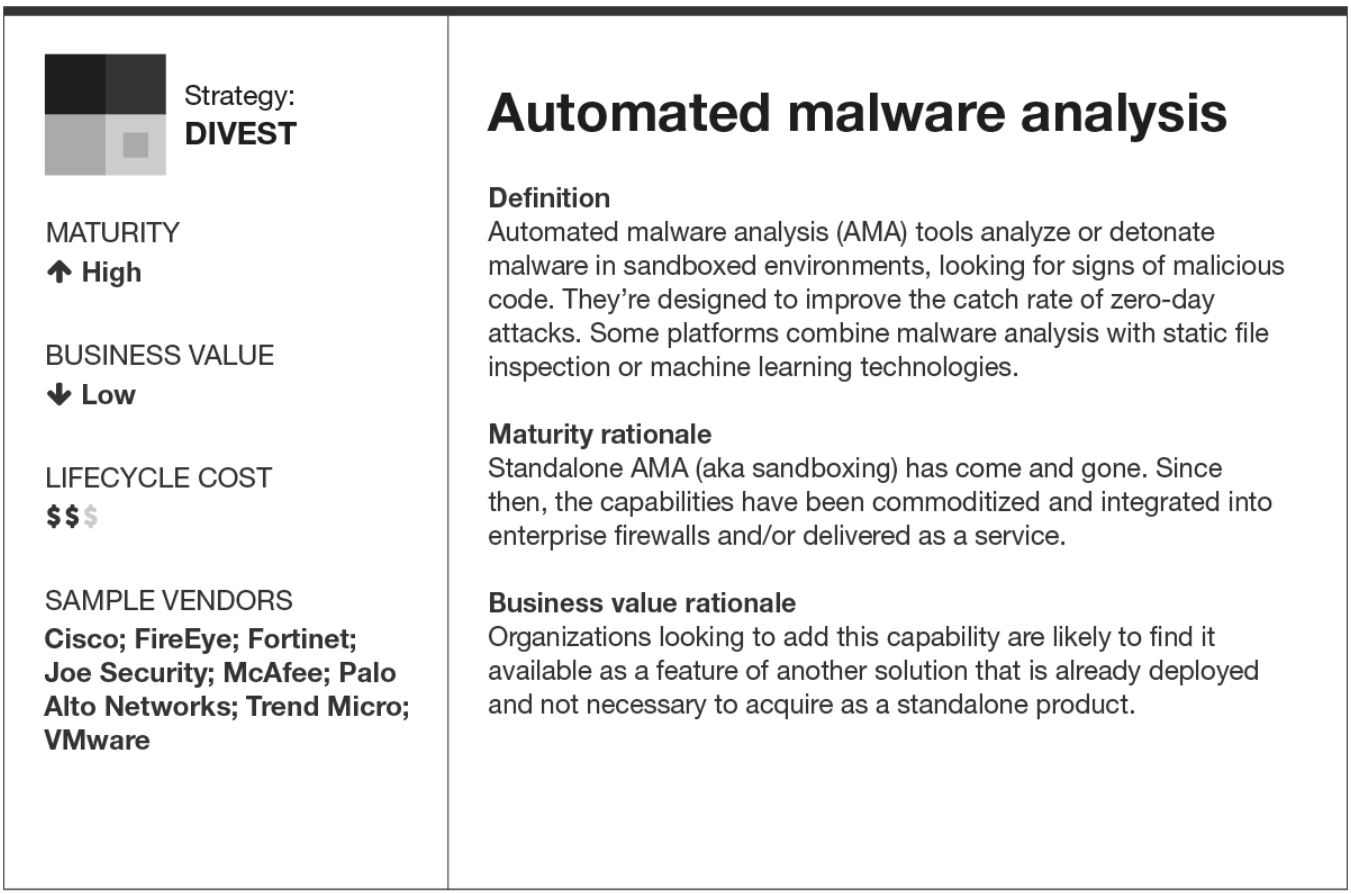
Five of the 17 technologies fall into the Divest quadrant of the Tech Tide, with high maturity and low current business value. When evaluating technologies in this category, keep in mind that they have already reached their business value ceiling or are no longer seen as a point solution but as a capability now commonly found in other detection and response tools or platforms. Before you decide to divest, review alternatives, and stick with a point solution only if there is a specific and critical detection or response need for your firm.

Automated Malware Analysis

Automated malware analysis (AMA) uses virtualized environments (sandboxes) that allow organizations to detonate potential malware samples in a safe environment, providing valuable information in the form of new malware samples to vendors. Vendors can then commoditize the intelligence into their products as improved detection. AMA as a standalone, on-premises appliance has declined in favour of integration with enterprise firewalls, email security solutions or, more recently, being offered as a cloud-delivered service (see Figure 14).

Figure 14

Divest: Automated Malware Analysis



Data Loss Prevention

Data loss prevention (DLP) suites help organizations identify and manage access to critical data, addressing multiple channels of data loss and furthering the centralized management of policies. Challenges include complexity of deployment, rule setting, alert fatigue, and manageability. Many of the suites have evolved to offer more than DLP (see Figure 15). Traditional DLP capabilities are also included in other product categories like enterprise email security and cloud security gateways, making it easier for organizations to acquire DLP as a feature. New deployment models (cloud-based) and techniques (deep learning) are emerging to improve functionality).

Figure 15

Divest: Data Loss Prevention

Strategy:
DIVEST

MATURITY
↑ High

BUSINESS VALUE
↓ Low

LIFECYCLE COST
$$$

SAMPLE VENDORS
Broadcom (Symantec); Digital Guardian; Forcepoint; GTB Technologies; McAfee; Proofpoint

Data loss prevention

Definition
Data loss prevention (DLP) tools detect and prevent violations of corporate policies regarding the use, storage, and transmission of sensitive data.

Maturity rationale
DLP is a common feature within other security offerings like email security and cloud security gateways and is built-in to Microsoft offerings. Traditional regex-based approaches that rely on DLP as a feature may fulfill the minimum for compliance. DLP as a feature will continue to advance in its detection and response capabilities, and suite providers have evolved their offerings to address compliance, intellectual property protection, and insider threats.

Business value rationale
While the ability to enforce policies for data movement — including blocking — can continue to be useful, businesses gain added value from integrated solutions that combine DLP with other functionality or enable protections that can move with the data.

Managed Security Services Providers

Managed security services providers (MSSPs) are third-party organizations that continuously and remotely manage and monitor security technologies for their customers. The four primary MSSP domains include, but are not limited to, perimeter and network security, application security, endpoint security, and identity and access management. MSSPs offer multitenant service delivery, automation, and a one-to-many support model to maximize economies of scale. MSSPs of all sizes are moving toward managed detection and response models (see Figure 16).

Figure 16

Divest: Managed Security Services Providers

Strategy:
DIVEST

MATURITY
↑ High

BUSINESS VALUE
↓ Low

LIFECYCLE COST
$$$

SAMPLE VENDORS
Accenture; Alert Logic; AT&T; Capgemini; Cognizant; Deloitte; ElevenPaths; EY; IBM; Kudelski Security; Lumen (formerly CenturyLink); NTT; Optiv; Secureworks; Trustwave; Wipro

Managed security services providers

Definition
Managed security services providers (MSSPs) offer expertise on demand across a wide portfolio of managed and monitored services. MSSPs use a multitenant delivery model and allow clients to gain access to a service that is far more sophisticated than one they could build on their own.

Maturity rationale
MSS is one of the oldest categories within the security ecosystem, and, as such, is reasonably mature. Significant disruption is hitting the market, as large and small MSSPs pivot to managed detection and response as a delivery methodology.

Business value rationale
MSSPs provide cost transference and labor arbitrage. Clients can avoid making sizable and costly investments in a 24/7 SOC. MSSPs never realized their aspirations of allowing clients to forego security teams in their entirety and, while some savings materialized, they never reached promised levels.

Network Intrusion Detection Systems

Network intrusion detection systems (IDS) have been around for decades, becoming an early technology for network threat detection. In recent years, enterprise firewalls have consolidated multiple security functions into one multipurpose security solution. Emphasis has also shifted from threat detection at the network edge to detecting threats on endpoints and in cloud environments. For many organizations, enterprise firewalls and network analytics and visibility (NAV) tools have replaced IDS (see Figure 17).

Figure 17

Divest: Network Intrusion Detection Systems

Strategy:
DIVEST

MATURITY
↑ High

BUSINESS VALUE
↓ Low

LIFECYCLE COST
$$$

SAMPLE VENDORS
Cisco; Fortinet; Palo Alto Networks; Trend Micro; VMware

Network intrusion detection systems

Definition
Intrusion detection and prevention systems (IDS/IPS) use signatures to detect and block malicious executables and network traffic.

Maturity rationale
One of the earliest network detection technologies, this market peaked years ago, and many security and risk professionals acknowledge that it failed to live up to its initial aspirations.

Business value rationale
While standalone IDS still has its place in some high-security environments, it's now more often utilized as an element of a threat detection and prevention stack within an enterprise firewall.

Security User Behaviour Analytics

Security user behaviour analytics (SUBA) solutions use behavioural analytics and machine learning to provide visibility across networks, devices, and applications. They are a principal technology for detecting insider threats. SUBA solutions were initially positioned as "SIEM helpers," providing additional detection capabilities based on suspicious behaviour. Since being introduced, many SUBA solutions have evolved into SA platforms or are being sold alongside DLP to provide additional context. As a result, SUBA's viability as a standalone technology is in doubt (see Figure 18).

Figure 18

Divest: Security User Behaviour Analytics

Strategy:
DIVEST

MATURITY
↑ High

BUSINESS VALUE
↓ Low

LIFECYCLE COST
**$**$$

SAMPLE VENDORS
Exabeam; Forcepoint; Gurucul; Haystax; Micro Focus; Rapid7; RSA; Securonix; Splunk

Security user behavior analytics

Definition
Security user behavior analytics (SUBA) enables security and risk teams to build a unified view of users' actions across the network. SUBA collects and correlates detailed information about user activity from a variety of logs and other data sources to heuristically and automatically set a user activity baseline from which it can detect, risk score, prioritize, and enable the investigation of anomalous behavior in real time.

Maturity rationale
These technologies are still nascent and are based on machine learning techniques and behavioral analytics. As a standalone technology, SUBA has not gained significant market traction.

Business value rationale
Understanding user behavior is only useful when combined with other technologies like DLP and identity. Security analytics platforms have built in SUBA natively, reducing the long-term viability of SUBA as a standalone product offering.

Supplemental Material

Methodology

The purpose of the lists of sample vendors we include in the figures about each category is to further clarify the nature of the category — not to serve as a vendor selection shortlist for readers seeking to choose a vendor in that category. The fact that a vendor isn't included in a list does not indicate that it isn't worth considering.