Cyber Resilience: A Framework for Minimizing Disruption

A Risk Management Approach to Protecting Data and Maintaining Business Continuity

EVOLVING SOLUTIONS

CONTENTS

Chapter 1: Introduction.....3

Chapter 2: Developing a Strategic Plan for Cyber Resilience..... 4

Chapter 3: Risk Management in the Digital Era: A Blueprint for Cyber Resilience..... 7

Chapter 4: Cyber Resilience and Data: Mitigating the Risk of Unauthorized Access, Theft, and Loss of Data..... 11

Chapter 5: Cyber Resilience for Identity and Access Management..... 15

Chapter 6: Cyber Resilience for Endpoints: Managing and Securing A Diverse Range of Devices..... 18

Chapter 7: Cyber Resilience for the Network..... 21

Chapter 8: Cyber Resilience and Attack Surface Management..... 24

Chapter 9: Cyber Resilience and SOAR..... 27

Chapter 10: Cyber Resilience and MDR/XDR..... 30

Chapter 11: How Evolving Solutions Can Help..... 33

Chapter 12: Working with Evolving Solutions..... 37

1. INTRODUCTION

Cyber resilience is the ability to adapt to any adverse condition to ensure business continuity, which includes the ability to withstand a cyberattack or recover from another type of unforeseen circumstance, such as a data center outage.

This e-book puts cybersecurity in context with an overall cyber resilience strategy designed to protect your valuable data if an adverse condition arises. We'll discuss the tools that help keep threat actors at bay, including tools for detection and response.

But the most important part of cyber resilience is the strategy for keeping the organization functioning despite a cyber-incident or other adverse condition.

A cyber resilience strategy reduces the chances of an adverse condition happening, and if something does occur — which, for cyberattacks, is a statistical certainty these days — a strategy will put your organization on a better footing to respond and restore operations quickly, minimizing disruption.

2. DEVELOPING A STRATEGIC PLAN FOR CYBER RESILIENCE

A FRAMEWORK FOR MINIMIZING DISRUPTION

If you've done your homework on how to detect and investigate incidents, you're in good shape to develop a strategic plan for resilience, because a strategy won't get you very far if you don't have the people, processes, and tools lined up to respond to an event.

While the tools and technologies give you the capability to detect and investigate, a validated cyber resilience strategy enables organizations to coordinate efforts and adapt to new situations, because even though incidents follow familiar patterns, the nature and tactics of threats are continuously evolving.

A STRATEGIC PLAN HELPS YOU ADAPT

Because every incident is unique, there's no way to have perfect playbooks that will work for every situation. By outlining the tactics, techniques, and procedures you'll follow in the event of an incident, and by outlining the responsibilities of the people who will be involved, you'll have a framework to respond to any event.

For example, first responders train for incidents but face unique challenges in the field. A complex incident may involve multiple agencies, such as fire departments, police, and ambulance services. These groups train together to sort out roles and responsibilities during an event and have invested in the tools and processes that will support their response. If something new happens, like a large brushfire that's threatening people and property, they may not have the exact steps at their fingertips, but they have a tested strategy to fall back on. An organization must approach cyber resiliency in a similar manner.

A STRATEGIC PLAN REQUIRES COLLABORATION

Because cyber resilience requires a holistic approach on how to anticipate, withstand, recover, and adapt to threats, it requires collaboration across the organization. It's not just an IT initiative where you buy redundant storage, invest in endpoint detection and response, or have multiple ISPs. The whole organization needs to understand the business need behind these investments and the impact on the organization if a group of employees isn't back to work quickly.

What technology does your warehouse team need to do its job in the event of an incident? Or your engineering group? Or your field crews? Or your executives? And what are the business priorities for recovery and restoration?

These conversations need to happen to have a strategic plan to support response efforts. The business requirements will shape the strategy and the strategy will point you in the right direction for making the right investments in the right resources.

TESTING AND EVALUATING A STRATEGIC PLAN FOR CYBER RESILIENCE

Once you have a strategic plan in place for cyber resilience, it needs to be tested and evaluated over time. Ongoing evaluations of your business impact analysis and regular tabletop sessions for incidents can help clarify roles and responsibilities during an event and will also help define priorities in restoring services.

You can also do regular disaster recovery tests to ensure your backup and recovery solutions work as expected when needed. Testing will help identify gaps in processes or tools and get newer employees up to speed on what response actions to expect within your organization.

Collaborative by nature, tests require input from throughout the organization — the different teams and business units that could be impacted by an incident. When an incident occurs, everyone has a role to play in restoring normal operations. So, a cyber resilience strategy goes beyond the IT department to include every aspect of the business that may be affected by an incident. A holistic resilience strategy must be supported and invested in throughout the whole organization.

Where to Focus

Many organizations like to test for ransomware, but it's not often the best place to start. While nearly all organizations face a risk from ransomware, the reality is other threats are more common, just not as headline-worthy. For example, a common zero-day vulnerability might lead to ransomware, or it could lead to other issues such as data exfiltration.

Another reason to test other scenarios is the behavior of one scenario is often similar to another. This allows you to test the tools and processes holistically. The tools commonly used to detect an insider threat are often the same tools used to detect lateral movement and data exfiltration commonly seen in ransomware attacks.

Start by focusing on top industry threats, such as business email compromise or account takeover. Evaluate these threats against your risk level and test there.

For inspiration on what to test for, read the news. Anytime a major newsworthy cyber event is reported in the media, run a mini tabletop. Pull the response team together and have a quick conversation. Talk about what happened and how a similar event might impact your organization.

For example, the MOVEit file transfer vulnerability made big news because so many financial and government institutions were using it to transfer highly sensitive information. Even if you don't use MOVEit, you should still have a conversation about the impact of a file transfer breach in your organization.

While many organizations test their plans fairly regularly, the evolving nature of risk and the inevitability of a cyberattack means tests should be conducted more frequently and on a variety of threats.

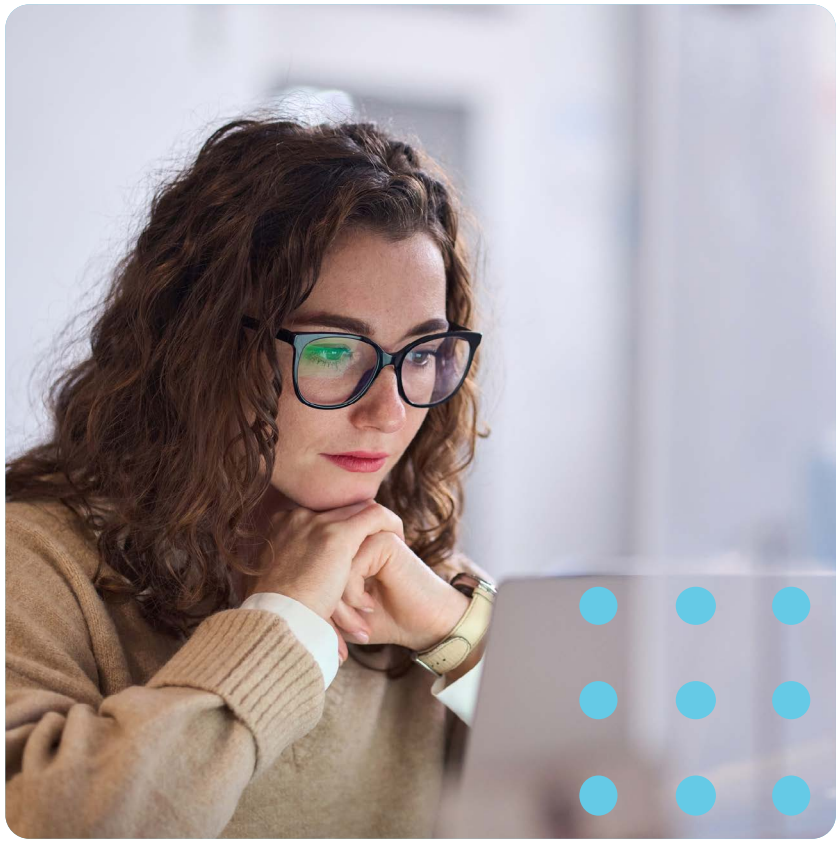
3. RISK MANAGEMENT IN THE DIGITAL ERA

A Blueprint for Cyber Resilience

Cybercrime continues to make headlines around the world, with the velocity and sophistication of attacks climbing to ever higher levels. It's happening in every industry, including the financial marketplace, healthcare entities, and other critical infrastructure sectors.

Ten years ago, an organization could temporarily go back to pen, paper, and manual processes to get by. Today, that's no longer realistic. In the last 10 years, and especially since the pandemic, business processes have become reliant on computer systems.

For example, in the event of a cyberattack on a hospital, nurses and physicians are still at work, but the pharmacy can't dispense medications without a computer and a barcode scanner, rendering patient treatment difficult at best. In the warehouse, the forklift still runs, but the location of items to pick is stored in a computer system.



COMPREHENSIVE PREVENTION TO ENSURE BUSINESS CONTINUITY

Security tools are important, but they don't guarantee freedom from successful attacks. In today's environment, an adverse condition is nearly inevitable. You can't count on cybersecurity tools alone to protect the business.

Cyber resilience is a strategy that focuses on keeping the organization functioning as best as possible during adverse conditions. Cyber resilience goes beyond technology tools to include an analysis to prioritize risks and develop response plans that mitigate damage from successful attacks.

Cyber resilience extends beyond traditional hacking, encompassing threats like disasters and social unrest. If a riot breaks out near your downtown data center, your cybersecurity tools won't be of much help.

Cyber resilience takes these realities into account. For example, by isolating critical systems such as the hospital pharmacy or warehouse inventory from business systems, the organization can continue to operate if adverse conditions manifest.

APPLYING FRAMEWORKS TO MINIMIZE RISKS

To stay abreast of best practices for cybersecurity, most organizations use popular security frameworks such as the NIST Cybersecurity Framework and CIS Critical Security Controls. However, the frameworks were developed more to guide tactics and less on creating a cyber resilience strategy. The frameworks are generalized remedies that don't take your organization's and your industry's unique risks and vulnerabilities into account. And frameworks don't help you prioritize risks to help you focus time and attention on the real threats to business continuity.

Many organizations end up using frameworks as checklists for implementing cybersecurity tools, checking the boxes as capabilities are deployed. Endpoint security? Check! Multifactor authentication? Check! Unfortunately, organizations that take the checklist approach are still dealing with catastrophic attacks.

Cyber resilience takes a different approach. It's about risk management.

A RISK MANAGEMENT APPROACH TO MINIMIZE IMPACT AND RECOVER QUICKLY

A risk management approach to cyber resilience requires CISOs and other IT leaders to understand how the organization makes money and how risks impact operations and revenue, because those are the risks that need to be protected.

Instead of focusing on the latest technology tools to secure the business, IT leaders need to focus on how technology risks impact the business. For example, a software company's risks are quite different from a manufacturer or healthcare provider. For a manufacturer, the risk of idle robots due to a cyber attack is big. No robots, no income. In the hospital, a computer failure can be a life-or-death matter. Software companies generally focus on protecting intellectual property. Strategies and tactics need to be specific to the threat landscape in your industry and your business.

Cybersecurity frameworks, and therefore checklists, don't take these realities into account.

Identify Critical Risks

A cyber resilience strategy starts with a risk assessment that identifies the most critical areas of the business and how the technology architecture supports them. Start by identifying the valuable data and other important assets on the network — assets that are critical to your most important processes. Because in the event of an adverse condition, IT leaders need to know which processes are critical and must be brought back to life first.

Then, you need a strategy to deal with the identified risks, which can be transferred, mitigated, or accepted.

Transferring risk generally happens by outsourcing cybersecurity to a managed security service provider or third-party security operations center. To mitigate risk, organizations can use the NIST or CIS frameworks for guidance, which is what they were designed for. In some cases, you can accept the risk because not every risk is critical. Organizations can choose to absorb the consequences if something goes wrong.

To evaluate a risk, do a business impact analysis of what would happen if a key capability suddenly became unavailable. You can even take an industry-specific approach to evaluating threats. For example, if there are threat actors targeting your industry with known tactics, you can implement protections to detect those tactics, and ultimately, develop processes to respond and recover.

Quantify Risk

In the event of a successful attack, organizations need to know which systems are likely to be impacted, their order or operation, the business function that's ultimately impacted, and at what level. The idea is to quantify the impact. Rather than merely describing the impact as "catastrophic," you should quantify the resources needed to recover.

By quantifying consequences, organizations can focus their cybersecurity efforts on leveling up maturity in areas that matter most. Basic controls may work fine for some systems. You may need to go deeper in higher risk areas. The cybersecurity frameworks provide excellent guidance for this.

Being proactive about quantifying risk will also help tremendously when it comes time to recover. The faster you can identify and contain an attack, the faster you can respond to minimize impact.

Develop a Culture of Resilience

Cyber resilience goes beyond the purview of the CISO, IT department, and legal and compliance departments. Every employee needs to know their responsibilities in ensuring organizational resilience. By bringing the organization together through tabletop exercises, you can begin to build a culture of resilience where everyone in the company knows their role in keeping the organization running at top speed.

4. CYBER RESILIENCE AND DATA

Mitigating the Risk of Unauthorized Access, Theft, and Loss of Data

In the past several years, data has reached new levels of importance and value as organizations become increasingly more reliant on data to run their business. This makes data resilience a top priority for these organizations.

While many organizations look to regulations and compliance frameworks to understand their data resilience requirements, data resilience requires a much more holistic approach. Data resilience must start with a deep understanding of the data your organization has, creates, and maintains, while also understanding the value of that data. Without a comprehensive understanding of your organization's data, it's difficult to know what to protect, how to protect it, or which regulations may apply. Good data resilience practices result in compliance, not the other way around.

Data resilience isn't just about regulated information either. In addition to regulated data, every organization has its crown jewels to protect. Product designs, trade secrets, and other intellectual property will be difficult to recover if lost.

Historically, people tend to think of data resilience as being synonymous with backups. However, in the modern world, data resilience expands beyond simply ensuring data is backed up to include protecting data as it's in use by understanding who needs access to data, when they need access to it, and how that data is protected throughout its journey. This includes retaining and purging data appropriately.

POTENTIAL CONSEQUENCES OF DATA LOSS AND BREACHES

The consequences of data loss and data breaches can be significant in terms of lost time, money, and reputation, especially if you're in a regulated industry or working with regulated data. Every organization processes some amount of personally identifiable information (PII), where a breach will result in fines and fees, which can be substantial.

Organizations are also at risk of reputational loss, even if the compromised data isn't regulated. If you expose a customer's or partner's trade secrets, it can erode your standing with existing and prospective clients. Most data legislation dictates that breached organizations must provide several years of identity protection services to individuals whose data was exposed, which is another potential cost.

Data loss and exposure can also significantly disrupt operations. If your crown jewels are compromised, can you even do business? This type of disruption is difficult to recover from and can result in the loss of clients and business.

Additionally, if a breach puts you in violation of contract terms, for example, being able to produce a certain number of components and equipment on time, the organization can be at risk of legal action.

COMMON GAPS IN THE PROTECTION OF DATA

In general, organizations understand the need to protect data that is known to be highly sensitive, but most organizations are not able to effectively identify and protect all data throughout its lifecycle within their environment.

While written security policies may direct employees to store sensitive data in a secure location, oftentimes, there's no monitoring or controls in place to prevent an employee from putting a sensitive document or spreadsheet in a less-secure file sharing platform.

Another common gap is data that doesn't have an owner — someone who's responsible for the information. Data that doesn't have a defined owner is hard to identify within the environment and difficult to understand who should have access to it. Therefore, it's difficult or impossible to adequately protect.

Taking a compliance-only approach as a data protection strategy has its gaps because if you don't know your data, you don't know what laws apply to it. In addition to HIPAA and GDPR, all 50 states have data privacy laws. If you're in Minnesota and keep data about customers in California or the European Union, you may be bound by regulations in those jurisdictions. It's not just one or two sets of regulations you need to follow.

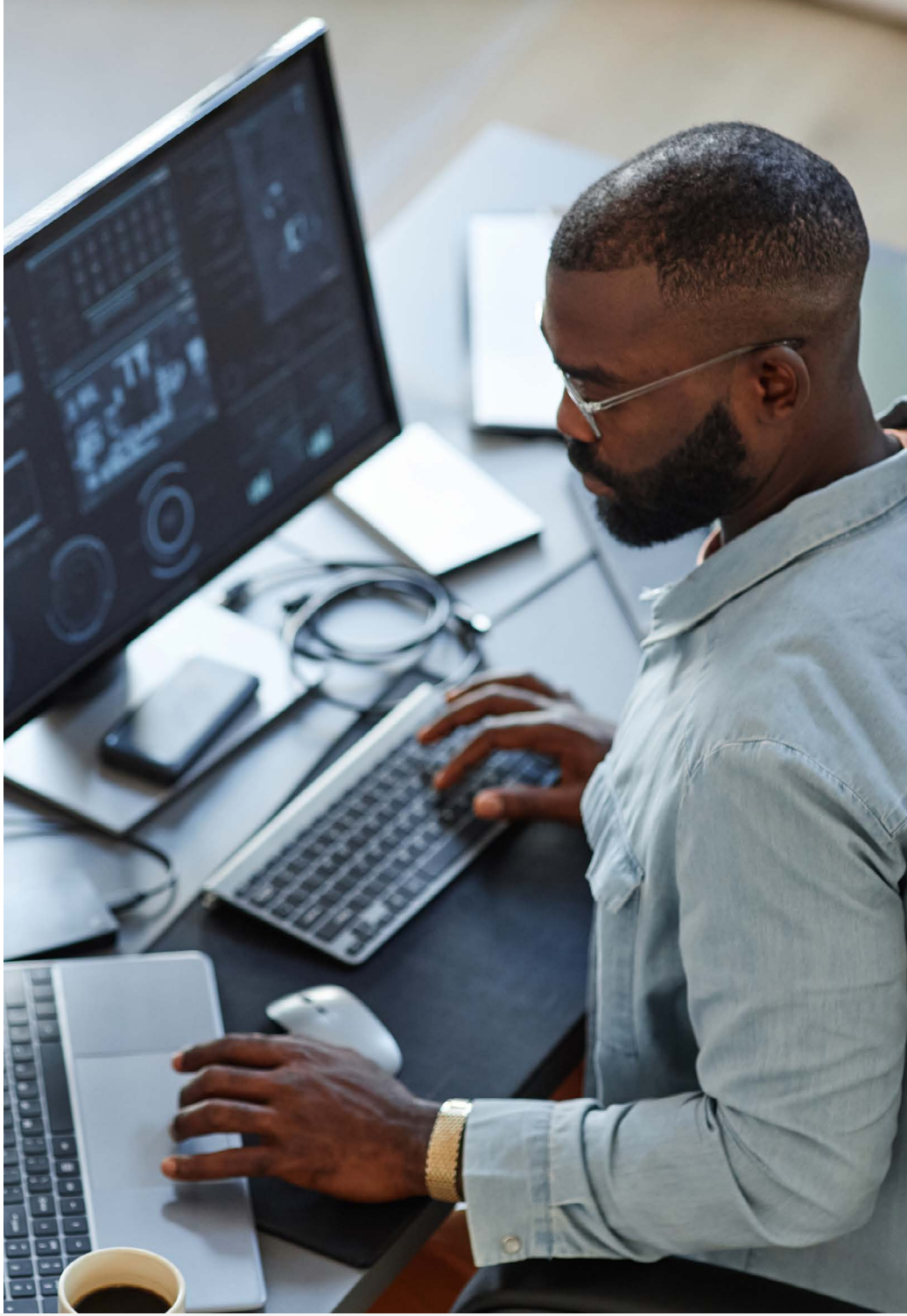
DATA DISCOVERY AND CLASSIFICATION (DDC)

Data protection becomes significantly easier when the location of data is known, and the data is classified. Data discovery and classification tools help organizations understand where data lives and the journey of data within your organization — the inflows and outflows of data — which is critical when developing a data resilience strategy.

There needs to be general agreement, from the executive level on down, as to what data exists in the environment and how it should be protected. This requires involvement from more than just your IT department. IT doesn't know the value or importance of specific data sets nor the people working with the data regularly.

The benefit of data discovery and classification — and mapping out the processes of how data gets created or ingested — is the ability to manage the lifecycle of data throughout the organization — protecting it in storage, protecting it in use, and purging data that's out of date.

Once you know where your data is and what it is, you can be more effective in determining what regulations the data is subject to and what controls to put in place to implement a data loss prevention solution effectively and successfully.

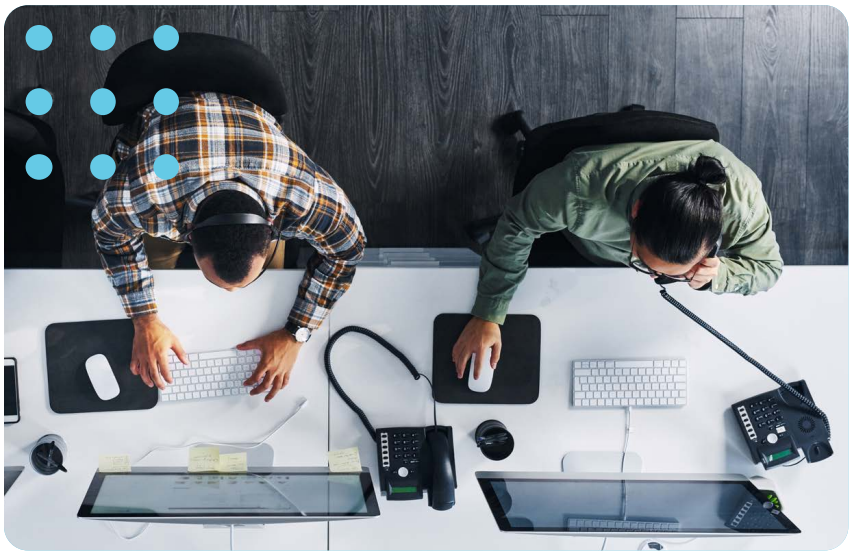


HOW DDC WORKS

Typically, DDC tools work by connecting to cloud and internal applications to crawl through file shares, workstations, laptops, and SaaS apps to discover information in your environment and classify data based on the content of data files. For example, if an HR database contains social security numbers, a DDC tool can categorize and monitor it to ensure that if an unauthorized user tries to access it, the organization can take action, whether it's to send an alert or block the activity.

Another aspect of DDC is end user behavior analytics (EUBA), which monitors how data is used by different roles throughout the organization. Anomalous behavior, such as a user opening thousands of documents at once, can be identified.

DDC isn't a one-and-done activity. It runs all the time to help ensure that the same data isn't copied across multiple locations. The DDC process may reveal that you have many more copies of data than you expected that are stored in inappropriate locations with the wrong people having access to it. This is a common scenario.



GETTING STARTED WITH YOUR DATA RESILIENCE PROGRAM

To get started on your own data resilience program, it's best to start with data discovery and classification. It's not necessarily an easy project. It requires having a plan for the upkeep, management, and tracking of data and the ability to classify data in real time or near real time. That's a hard pill to swallow when you're knee deep in other security projects.

But it can be worth the effort because when you know your data, you can start to shape priorities around next steps for data security because you have better clarity on what to protect and what's subject to regulation.

5. CYBER RESILIENCE FOR IDENTITY AND ACCESS MANAGEMENT

User identities — we all have more than one in the digital era. User identities are what enable users to access corporate systems and conduct their day-to-day job functions. However, it's these same identities that attackers take advantage of to execute attacks within your environment. The latest threat reports show that the majority of modern attacks — from ransomware, data exfiltration, fraud, and more — leverage identities at some stage of the attack.

Because of the significant use of identities in these attacks, organizations must take care to appropriately secure identities within their environment. Protections go beyond simply managing usernames and passwords or adding multifactor authentication. Identity management expands these security controls to include access certification, which is the process of identifying access needs for employees and third parties, such as vendors and partners, based on their role or function and ensuring each user is granted just-in-time access and permissions to only the information and resources they need to do their work.

When prioritizing cybersecurity initiatives, developing the tools and processes for protecting identities should be at or near the top of the list given the criticality in cyber resilience. When organizations dial in and standardize processes for protecting identities by defining access around roles and activities, they reduce the chances of identities, and subsequently, other protected assets, from being exposed.

COMMON RISKS TO IDENTITIES

When securing identities, most organizations focus on, and therefore implement controls around, external threat actors. Because of this, overly permissive entitlements often go overlooked leading to more impactful incidents when they do occur. For instance, how many people have access to HR information that shouldn't have it? Or client information for clients they never work with? If you're not monitoring this type of access, the answer is probably more than you realize. Or how often does someone drop sensitive files into a less secure location such as a department file share? It happens a lot more often than organizations like to admit.

Prioritizing and enforcing least privilege access with just-in-time access to data goes a long way in protecting sensitive information from accidental, unauthorized access by insiders.

VULNERABILITIES AROUND IDENTITY AND ACCESS MANAGEMENT

Most identity and access management (IAM) vulnerabilities are related to improper configuration, a lack of visibility, poorly defined processes, or a breakdown in processes.

Not Keeping Up with Organizational Changes

One of the biggest challenges we continue to see in most environments is excessive permissions accumulated over time, usually by more tenured employees. As roles evolve, employees typically get access to new resources. Over time, this may result in access to a significant portion of the company's information and data.

Overly permissive identities widen the scope and impact of an attack. Good IAM practices ensure that a user's scope of information is limited to the needs of their role and regularly evaluated for any deviations. Organizations need processes in place to ensure that joiners (new employees) and movers (employees changing roles) have access granted or revoked based on their evolving role in the organization. Leavers (employees exiting the organization) also need a process as they are quite often overlooked.

Organizations should also consider defining or optimizing processes to address these common scenarios that can lead to identity exposure:

- A new employee fills a new role that's not fully defined. In many cases, organizations grant too much access just in case they need it.
- An employee needs temporary access to new information, for example, to support a special project or to cover for someone who's sick or on leave. In this case, it's important to put a time limit on access.
- Temporary elevated access for IT staff during troubleshooting should be approved, reviewed, and only granted for a limited amount of time.
- Machines and processes that use credentials for system access, especially with elevated privileges. This scenario is increasingly common in Modern Operations environments where infrastructure is consistently evolving.
- Users with global read-only access to databases. While it may seem like overkill to set up a limited read-only account, it is worth it as it limits exposure if a bad actor gets access to the account.

Excessive Session Times

When organizations configure their IAM platform, it's not uncommon for some out-of-the-box defaults, such as session timeout limits, to not be configured to best practices. Or possibly some number

of accounts are exempted from these configurations without appropriate review of risk due to company culture or system limitations.

Session times should be determined using a risk-based approach based on role, function, and intended activities. For instance, when you invite users to click a checkbox at login to remember their credentials, should that privilege be granted forever for everyone in each instance? For those on the go, an hour may be the best timeframe for remembering credentials because that's how long they're likely to be in one location.

By putting some real thought into customizing session times based on roles and activities, you can reduce the risk of exposing credentials.

Not Protecting Your IAM Platform

Because identities are the keys to the kingdom, threat actors will often work to escalate permissions once they have a foothold in an environment. One way they can do this is by targeting and compromising the underlying security authentication system: your authentication platform.

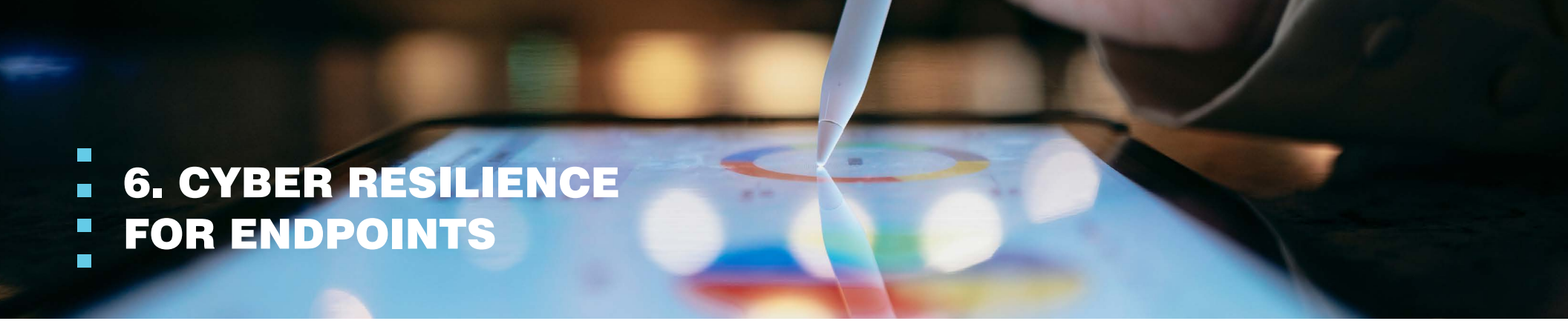
One such technique was used by bad actors during the SolarWinds incident in December 2020. For months prior to public disclosure of the compromise, threat actors were utilizing the "golden SAML" attack within environments, allowing them to impersonate any user, bypass MFA requirements, and ultimately make it much harder for security teams to detect.

Lateral Movement in the Event of a Breach

The goal of cyber resilience is to minimize the exposure and impact of an attack, which includes limiting the "blast radius" if a breach does occur. With proper tools and controls in place for IAM, a breach can be less costly to the organization. While other resilience techniques such as endpoint protection are important, protecting identities and access is critical to preventing unauthorized lateral movement to other systems within the environment. Good IAM management is the best control point for preventing lateral movement and limiting the blast radius of a successful attack.

Getting Locked Out at an Inconvenient Time

While building and improving processes to protect your identities, it's crucial to consider the entire lifecycle of an identity. While that includes the joiners, movers, and leavers, identity plays a role in incident response and recovery as well. While administrative use should be limited, incident response teams must also take into consideration what accounts and permissions they may need access to during incident response. Processes must be designed to ensure authorized users are not completely locked out of your systems.



6. CYBER RESILIENCE FOR ENDPOINTS

Managing and Securing a Diverse Range of Devices

With the advent of remote work, endpoints have become a rich target for cyberattacks. While traditional protections such as antivirus software, patching, and endpoint detection and response (EDR) are important, they don't fully address today's risks.

A threat actor can learn a lot about your environment and processes by getting access to an endpoint. Once an endpoint has been compromised, attackers can move laterally through the network and gain access to critical resources.

While most organizations do a good job of protecting known, "trusted" devices such as company-managed PCs and laptops running on the company network, there's plenty of activity coming from "untrusted" personal devices.

Smartphones and tablets are inherently more difficult to secure because some of the functionality available on workstations isn't available on these devices. For example, users can't hover over links on a phone and employees who let their guard down for a moment may click on a dodgy link in a text message or email. Yet, today's workforce expects the flexibility to use personal devices to access files, attend online meetings, receive and respond to emails, and conduct other business.

YOU CAN'T PROTECT WHAT YOU DON'T KNOW ABOUT

At this point, most organizations are using EDR because it helps IT teams identify and contain events and provides deeper insight into the context of what's happening at the endpoint: what processes are running and what the user is doing.

But EDR doesn't provide holistic visibility into what endpoints are active, their configuration, health, OS and software versions, patches, and which devices are managed by the organization and those that aren't.

Since you can't protect what you don't know about, you can't respond to an event on an endpoint you don't know about. In essence, without comprehensive endpoint visibility, you're leaving the front door open.

IMPROVING ENDPOINT SECURITY FOR BETTER CYBER RESILIENCE

The challenge for IT teams is to enable the flexibility for employees to use untrusted devices for work while minimizing threats. To do that, endpoint security must go beyond patching, antivirus, and EDR to include centralized mobile device management, deeper visibility into every endpoint, and hardening security for company-managed devices.

Hardening Device Configurations

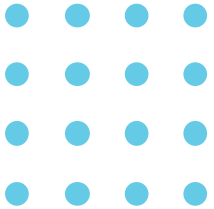
The best place to start in improving endpoint resilience is with initial device provisioning. Unfortunately, many organizations don't consistently roll out hardened baseline configurations for their new Windows PCs, Macintoshes, and other devices. This leaves the door open for threat actors because they know what the manufacturer's default configurations are and use them to launch exploits.

Before they're shipped to users, devices should be provisioned using a standard image that's hardened to ensure that unnecessary services are turned off and critical resilience features like encryption are turned on. Doing this manually will inevitably lead to missed steps and unnecessary exposure due to inconsistent configurations, so the provisioning process should be automated as much as possible using services such as Microsoft Intune and Windows Autopilot.

Consistent provisioning also improves cyber resilience by providing a more consistent experience for IT teams to enforce standards and troubleshoot issues. In the event of an adverse condition, IT teams have a quick, consistent method of drilling down to remediate an issue, whether it's using EDR to isolate a device, running vulnerability scans, or patching where needed.

Centralizing Device Management with MDM

The next step in improving endpoint resilience is having a centralized device management platform that supports both company-managed and personal devices. Mobile device management (MDM) platforms give IT teams visibility into desktops, laptops, smartphones, and tablets to manage tasks like patching and software updates and enforce policies and restrictions.



IMPROVING ENDPOINT VISIBILITY

One of the biggest challenges in protecting endpoints is a lack of centralized visibility into what devices are on the network. Without visibility into device activity, you don't have the ability to detect if something malicious is happening. With centralized visibility, the challenges presented by personal devices are minimized.

Centralized visibility collects device information from multiple tools to provide quick, easy-to-access information and context on every device connected to the network. This helps IT teams better understand vulnerabilities in devices connected to the network, including applications running and accounts being used.

Cyber Asset Attack Surface Management — CAASM

An emerging approach to centralized endpoint visibility is cyber asset attack surface management (CAASM), which enables IT teams to overcome challenges to asset visibility and exposure. CAASM gives IT teams quick, consistent visibility into all endpoints across your environment by pulling information from all your management tools, including MDM, cloud services, and network management tools. Once you know what's out there, you can protect it.

CAASM shows what protections are in place on every endpoint. For example, it will show if there are endpoints that don't have antivirus or EDR installed or if the configuration of a device is hardened to organizational standards. It also gives IT teams the ability to scan a device for vulnerabilities.

CAASM helps identify these types of gaps a lot faster than individually going into MDM, EDR, and other management solutions to pull information and manually compare lists. It's always easy to miss something when relying on manual processes.

7. CYBER RESILIENCE FOR THE NETWORK

IT has seen a lot of change in the last five years, but few things have changed more dramatically than networking. Unlike in the distant past when everyone connected to on-premises resources from the company network, today's networks handle a significant amount of traffic from remote workers.

This has expanded the scope of concern for IT professionals who are challenged to protect more devices in more locations. In this environment, networking professionals must think about how they can ensure that the protections in place for in-the-office workers on the corporate network can be provided for remote workers as well.

In addition, hybrid cloud environments have made networking — and securing the network — a bigger challenge. Because the network is a component of everything in the computing environment, a secure network is crucial to overall cyber resilience.

LIMITING ACCESS WITH PATCHED FIREWALLS AND POSTURE SCORES

The last few years have seen a massive increase in the number of organizations suffering cyber incidents from firewall vulnerabilities being exploited, enabling access into the environment. Minimizing vulnerabilities should be a key priority in shoring up the cyber resilience of the network.

Switches and firewalls should be regularly updated with the latest patches to ensure the vendor's latest security features are in place. In addition, switch and firewall configurations must be regularly maintained to ensure they meet standards.

Another way to limit access is with posture scores. By feeding endpoint data into network security tools, network teams can set rules around who gets access to data. The score can be based on a user's identity, location, the quality or health of the endpoint

in terms of patches, software updates, and whether antivirus or endpoint detection and response (EDR) tools are installed. Devices with a low score can have network access limited to basic functions such as email and collaboration to keep the organization's crown jewels safe. Location is a key consideration. Public wireless access from places like coffee shops are high risk and could warrant limited access.

LIMITING LATERAL MOVEMENT WITH NETWORK SEGMENTATION

The most successful cyberattacks rely on lateral movement through the network to gain access to and exfiltrate data. One of the primary goals of network security is to limit lateral movement and data exfiltration in the event of a successful attack.

From a security perspective, network segmentation is critical because it's the best way to limit at-will lateral movement for threat actors through the network. The more you can restrict lateral movement through segmentation, the less exposed your data is to exfiltration. Smaller containment zones lead to better resilience. It's a bit like your house. In addition to locks on the front and back doors, you can also lock doors to rooms to limit the movement of an intruder and their ability to take something.

Most organizations are at the point where the internal doors are in place, but the locks aren't. It takes a lot of planning and time to lock these segments down, which is why many organizations haven't had the opportunity to do so.

ENABLING VISIBILITY TO DETECT ANOMALOUS BEHAVIOUR

One thing many organizations lack is visibility into network activity. Without visibility, it's nearly impossible to determine if a bad actor is at work in your network and what they're up to.

With better visibility into the network, IT teams can detect anomalous behavior and see what data is moving around the environment, what's coming in from the outside, and what's moving from the inside out.

The NIST Cybersecurity Framework (CSF) provides helpful guidance in developing a resilient network. However, meeting the NIST framework objective goes beyond having the tools in place. It requires configuring and implementing the tools correctly to help you understand your network traffic — who's allowed in and who's not. More specifically, NIST recommends having the ability to monitor network traffic to block inappropriate activity and allow authorized traffic.

MODERN TOOLS TO MONITOR NETWORK TRAFFIC

There are several tools available to improve network resilience, most of which have emerged over the last five years to meet the needs of remote work and hybrid cloud environments.

Intrusion Detection and NDR

Intrusion detection systems detect suspicious activity to catch threat actors before they do damage. Intrusion detection systems enable network teams to put rules in place to limit access to network segments and get visibility into anomalous activity, such as an unauthorized user trying to access the network. Intrusion detection is like putting a Ring camera in every room of the house, giving you a documented trail of an intruder gaining entry, moving around the network, and possibly taking data outside the network.

In addition, network detection and response (NDR) systems apply behavioral analytics to network traffic to detect abnormal network behavior.

Secure Access Service Edge (SASE)

Another popular network security tool is secure access service edge (SASE), which consolidates multiple security functions such as secure web gateways, cloud access security brokers, and firewall as a service to reduce complexity and improve speed and agility for software-defined networks.

SASE delivers security controls as a cloud service to the source of the network connection rather than a data center, gives network teams visibility into every network request, and enables them to apply policies to the data in each request.

NOW'S A GOOD TIME TO REVIEW YOUR NETWORK ARCHITECTURE

Because networking has seen more change in the last five years compared to the 10-20 years prior, now is a good time to have conversations about the architecture and design of your network, especially in light of the consequences of not doing so. Once something malicious gets into an endpoint, it can run everywhere inside the network if proper controls and tools aren't in place.

By taking a step back and evaluating your entire network infrastructure, you can find new and effective ways to incorporate resilience into your network, such as intrusion detection, NDR, and SASE, which extends network and firewall capabilities to cloud resources so organizations can start treating cloud resources in a similar way as they handle on-premises resources. Legacy tools and processes for network connectivity and resilience simply don't have these same capabilities.

While network segmentation and containment aren't new concepts, the technology for enabling segmentation and containment has improved to make it much easier and more effective to implement. By creating opportunities to add visibility to the front doors of your data center and cloud providers, network administrators will be on a better footing to find and react to adverse network conditions.

8. CYBER RESILIENCE AND ATTACK SURFACE MANAGEMENT

Before digital transformation — or what we like to call "business transformation" — the attack surface was relatively static and well understood. But with the advent of remote work, digitized business services, and the mass adoption of IoT devices, the attack surface has become fluid. Any change in the way you operate your business changes the attack surface, including every new remote user, business service, device, and business location.

IBM defines the attack surface as, "The sum of vulnerabilities, pathways, or methods (attack vectors) hackers can use to gain unauthorized access to the network or sensitive data, or to carry out a cyberattack."

While the attack surface includes both internal and external resources, there's usually an emphasis on your publicly facing presence such as a website or applications. Until now, it's been difficult to get an accurate picture of the attack surface as it changes.

ATTACK SURFACE MANAGEMENT: A NEW APPROACH TO IDENTIFYING VULNERABILITIES

Attack surface management (ASM) is a relatively new concept that ties together existing tools and functions to give security teams a view of the environment from the attacker's perspective — from the outside in — to determine if a threat actor has a path into your environment and the ability to penetrate deeper.

ASM supports a modern approach to asset management by giving you the ability to continuously identify known and unknown assets as well as analyzing, prioritizing, and remediating vulnerabilities and other potential attack vectors. This approach imitates techniques used by threat actors as they target an organization.

Organizations already know where their crown jewels are and typically implement firewalls, endpoint detection and response (EDR), or other defenses to protect them. But every environment

has some level of public-facing presence, such as a website or applications, which are key targets for attackers while conducting reconnaissance to map out your public points of presence. Failure to manage the attack surface can expose your organization to fraud, ransomware, insider threats, data exfiltration, and other threats.

Continuous Monitoring of the Attack Surface

Prior to the emergence of ASM, activities around managing the attack surface have been point-in-time snapshots. ASM brings continuous monitoring into the equation, tying together vulnerability management, asset management, and open source intelligence (OSINT) to continuously monitor changes in the attack surface.

OSINT is a library of publicly available information, which may include your public IP addresses, leaked passwords, and other valuable information that hackers can access and use to plan attacks. ASM leverages OSINT so you can know what hackers know. OSINT information is sourced from the web, including uncrawled information (deep web) and the dark web. The industry consensus is that deep web and dark web information comprise about 96% of all information on the internet, so you won't find it on search engines.

ASM enables you to monitor the attack surface as it changes. Historically, organizations inventory and scan their IP addresses for vulnerabilities. ASM can manage this for you.

Processes are More Important than the Tool

Like any security tool, it's only as good as the processes that support it. ASM doesn't remediate, so you'll need processes to act on ASM feedback. ASM generally automates asset discovery, classification, and prioritization of asset vulnerabilities. But it also may generate new processes, which may or may not be automated, depending on your situation. You may need to trigger a playbook within your patch management system or SOAR platform to act on findings from your ASM tool.

WHAT YOU CAN EXPECT FROM ASM

Discovery of More Vulnerabilities than You Imagined

One thing that ASM can draw attention to is the amount of OSINT information that exists about your organization. This is vitally important because for the first time, you'll know the basics about what hackers know about your environment. The results can be startling. For example, ASM can surface a remote server exposed to the internet along with previously unknown admin credentials, which together form an attack chain where the credentials are used to log into the server to get into your environment.

Discovery of Unknown Assets

You may be surprised at the number of unknown assets exposed to the public. If your company was involved in a merger or acquisition, you may have dormant accounts that can be compromised. Or you may find a shadow IT cloud presence that's storing sensitive information. It's also possible to find malicious assets that an attacker has placed in your environment such as software or devices. An attack like this made headlines when a cloud hypervisor tool was used to create virtual network interfaces and a socket-type network device to connect to a remote server, bypassing firewalls, and intrusion detection.

A More Proactive Stance Against Attackers

In terms of overall resilience, ASM can give organizations a more proactive stance against threat actors by identifying gaps and weaknesses before they're used as a gateway to an attack. As a result, organizations can close more vulnerabilities faster as ASM surfaces issues. Overall, your organization should be less vulnerable to an attack, or in the event of an attack, get actionable information sooner rather than later.

What ASM Doesn't Do

ASM doesn't replace the need for traditional penetration testing and red team tests. It fills the gaps between your routine point-in-time tests.

9. CYBER RESILIENCE AND SOAR

Threat actors have stepped up the pace of malicious activity. Not only has the number of attacks increased, but the time it takes for a breach to turn into a business problem has narrowed significantly from months or weeks to days or even hours.

So, when it comes to responding to a breach, faster is always better. The early decisions made when responding to a potential security incident can make the difference between successful containment and a crisis.

Manual processes for responding to a breach generally involve a security analyst getting assigned a ticket or seeing an alert, which takes time. The analyst would then manually access the security tool that initiated the alert and pivot to other tools to investigate, which takes more time. It's also possible that an alert simply doesn't get a response, depending on the analyst's workload.

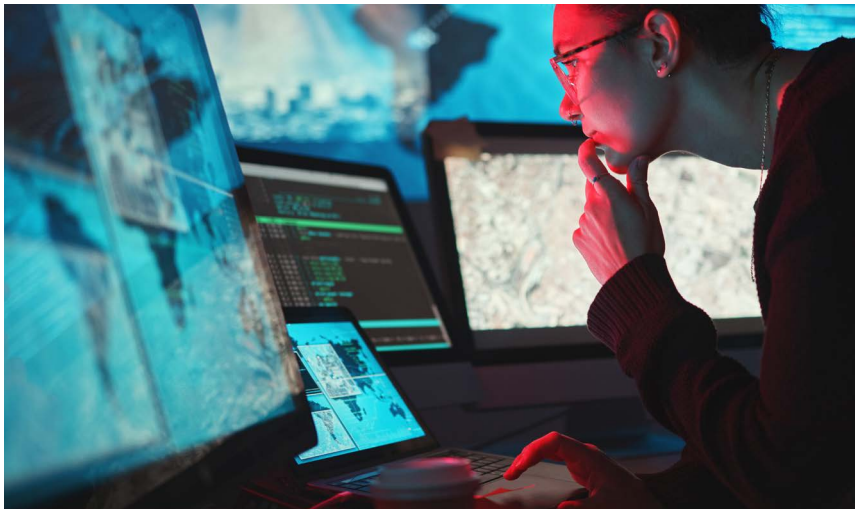
Given the high stakes involved — downtime, data exfiltration, revenue loss, and reputation damage — and the compressed time from an attack to a significant impact, manual processes are too slow, giving threat actors time to penetrate further into your systems and data.

The key to success is automation — the ability to contain a threat without waiting for human input. Security orchestration, automation, and response (SOAR) is a relatively new way to automate response processes. What took minutes, hours, or even days in the past using manual processes can now happen immediately with SOAR, which can contain the blast radius of an incident before a human analyst can get eyes on the system.

INVESTIGATE AND RESPOND TO ATTACKS IMMEDIATELY

SOAR is somewhat like a 911 call center. You may need the fire department, or the police department, an ambulance, or a combination of all three. The 911 dispatcher helps determine the necessary resources to dispatch based on the type of situation and orchestrates the process of getting the right people and resources to the right place.

Like the 911 dispatcher, SOAR doesn't detect, respond, or remediate. It's the tool used to orchestrate your security resources to respond to an event. SOAR closes the gap between an attack and your response. As soon as detection happens, SOAR can kick off automated playbooks to act before an attack turns into a full-blown security incident.



SOAR ORCHESTRATES TOOLS, PROCESSES AND PEOPLE

SOAR queries information from multiple security systems such as EDR (endpoint detection and response), NDR (network detection and response), XDR (extended detection and response), SIEM (security information and event management), and more, giving security analysts visibility and context around an event. It orchestrates resources using automated playbooks and processes such as taking action to isolate an endpoint or update a firewall rule. Automation ensures the right steps are taken in the right order.

SOAR can also trigger remediation actions or hand the incident off for human input, for example, if your backup and recovery team or legal team needs to get involved. SOAR can also orchestrate system recovery or help restore systems from backup.

SOAR helps security analysts investigate an attack by providing visibility — a single view of an attack and how SOAR is orchestrating a response. SOAR's improved context, combined with orchestration and automation, can lower the mean time to detection and speed up the mean time to respond. By detecting and responding to threats more quickly through automated playbooks, the deleterious effects of an attack can be contained and mitigated.

PUTTING SOAR IN CONTEXT

While SOAR can potentially reduce the impact of an attack, it's not a standalone system or a super-solution. SOAR doesn't replace existing detection and event management technologies but complements their value by centralizing event information for high-level visibility and context.

It also doesn't replace security personnel. Security professionals need to be available to fill in the gaps and make decisions as necessary, depending on the situation. But by automating workflows, security analysts will spend less time investigating. In this way, SOAR is a force multiplier that gives security analysts more breathing room to better understand the nature of an attack and ensure that automations are running as planned. It also gives Tier 1 analysts more time to write playbooks and automations because their time isn't absorbed with incident response.

Perhaps SOAR's biggest benefit is peace of mind. To the extent that security analysts can trust the automations, they can sleep better at night knowing that if sleep is interrupted by an incident, SOAR is already working on the issue.

WHAT YOU NEED TO MAKE SOAR SUCCESSFUL

What generally holds organizations back from getting value from SOAR is a lack of well-defined processes for responding to attacks. At Evolving Solutions, we've found that many organizations simply don't have the time to develop detailed response plans for likely scenarios.

It's impossible to automate something that doesn't have a defined process, so SOAR can only provide value when well-defined processes are in place. For example, processes define how SOAR should respond to specific types of detections and are the basis for the actions, the order of steps, and the data and resources required to contain an event.

10. CYBER RESILIENCE AND MDR/XDR

Threat actors have many ways to attack and compromise systems, and cybersecurity vendors have responded with multiple solutions to detect and respond to attacks. For example, solutions such as endpoint detection and response (EDR) are crucial for helping security teams identify attacks on an endpoint.

But what happens when an attacker circumvents your endpoint controls and manages to move laterally through your network? As alerts cascade in, security analysts want a full view of the attack. But pivoting between tools is time consuming — generally slower than the pace of the attack.

This is where extended detection and response (XDR) comes in. XDR consolidates input from multiple security technologies to provide visibility into an event so that security teams can track an attack as it unfolds.

Of course, security professionals are already busy building their security infrastructure, developing playbooks and automations, and generally working to ensure the organization is robust to an attack. So, when a breach does occur, they must pivot away from this work to investigate.

This is where managed detection and response (MDR) can help minimize the amount of time your team spends investigating. As the name suggests, MDR is a managed service that uses highly experienced and specialized security analysts to monitor your security platforms to respond to events surfaced by XDR and other detection and response technologies.

HOW XDR WORKS

XDR is a highly versatile solution that consolidates intelligence from multiple, disparate security technologies to provide comprehensive visibility into events that span endpoints, identities, data, the cloud, and networks for a correlated, birds-eye view of an attack across your on-premises and cloud footprints.

When implementing XDR, most organizations start by ingesting and correlating endpoint and network events and potentially expand the scope to include identities, data, and other systems. So, instead of only getting visibility into endpoint detections, or only network detections, XDR combines and integrates detection technologies to see how an attack unfolds over time. For example, you could see a compromised user account, which led to lateral movement on the network.

XDR is often supported by AI to help correlate events and build event timelines. Response to XDR alerts can often be fully or partially automated by security orchestration, automation, and response (SOAR).

Most security vendors offer an XDR solution, usually as part of a larger platform that can include EDR, NDR, SIEM, and SOAR, and may also include an MDR component.

HOW MDR WORKS

Security events don't always happen during business hours, and many organizations don't have the resources to run a fully functional security operations center (SOC) to respond to alerts at night, on weekends, over holidays, or to cover for someone on vacation.

MDR is a way to outsource SOC capabilities to have experienced security specialists watching your systems 24/7 using consistent, proven processes to respond to alerts on your behalf. This extensive coverage helps ensure that events are triaged as they surface.

The MDR team takes tailored actions as agreed upon by your organization and reaches out to get your team involved only when necessary. This can significantly cut the workload for security analysts who are often already busy developing architecture, rolling out services, optimizing existing services, and writing playbooks and automations. MDR gets your security team out of the disruptive grind of responding to every alert.

MDR augments your security team so the team can focus on moving the company forward rather than investigating alerts that may or may not be legitimate threats to the organization.

MDR OFFERS EXPANDED THREAT INTELLIGENCE

In addition to continuous coverage, outsourced MDR teams are experts at responding to alerts and events. That's what they do all day. They work for multiple companies in multiple industries and organizations of different sizes worldwide, so they see a lot. They can correlate attacks in process in multiple organizations or across an entire industry. This wide-ranging, real-time perspective gives them access to threat intelligence that's simply unavailable to internal security analysts.

Overall, MDR can give organizations a more proactive security stance, enabling them to catch and remediate attacks faster to minimize disruption.

MDR can work in a couple of different ways. Your MDR provider can hook into your existing security solutions or you can simply hook into theirs. It depends on what the provider offers and what requires augmentation on your end.

GET CLARITY ON YOUR MDR RELATIONSHIP

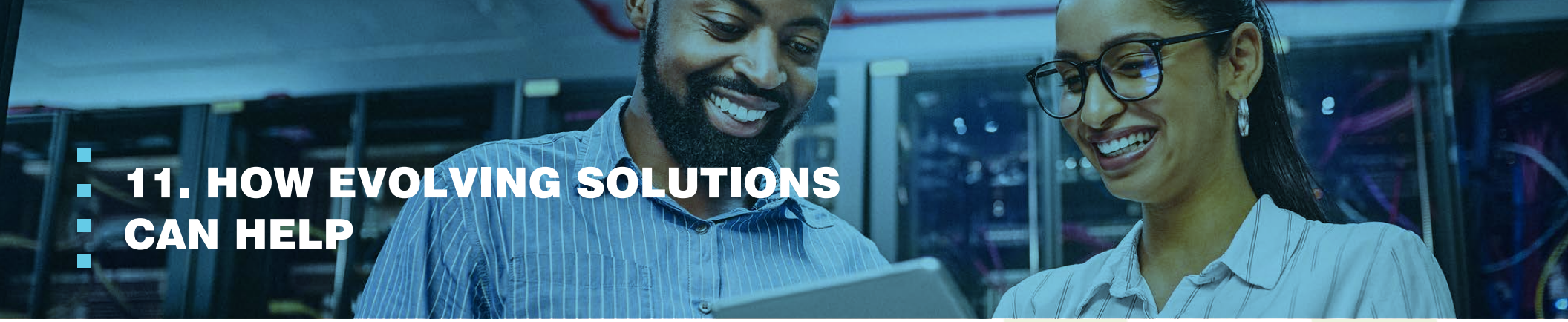
The most important thing about developing a relationship with an MDR provider is to get clarity on where the MDR provider's responsibilities begin and end. It's important to understand what your MDR provider is doing for you because if an event occurs, personnel on both sides may need to get involved. You'll want a clear picture of how that will work before an attack occurs.

It's also important to have performance metrics for your provider so you know they're doing what you expect them to do.

WHAT YOU CAN EXPECT FROM XDR AND MDR

With XDR and MDR working together, event response times should be faster. The comprehensive visibility that XDR provides into your detection platforms also gives security teams a higher level of confidence that investigations and remediations actually address the issues you're trying to solve. In the event of a ransomware attack, you'll be able to, for instance, trace a compromised user account to specific files accessed by that account to see the entire scope of an attack.

In contrast, without XDR, you may know what triggered an event, but you may not get the full scope of accounts or data involved in the attack. And without MDR, your response may be slow or limited in scope.



11. HOW EVOLVING SOLUTIONS CAN HELP

EVERY ORGANIZATION IS UNIQUE

Every organization is unique in terms of its business opportunities, operations, and risks. While general advice can help you better understand how to improve cyber resilience, you can benefit from partnering with an experienced partner that has an approach that puts cyber resilience in context with your business objectives, technology stack, and risk profile.

GET THE MOST FROM YOUR EXISTING TOOLS

While many organizations have the right technology in place for cyber resilience, many haven't been able to invest the time needed to build robust processes around that technology. Evolving Solutions can help you get the most from your security investments and better utilize the technology investments you have already made.

HOW EVOLVING SOLUTIONS CAN HELP

Cyber Resilience and Data

Data discovery and classification (DDC) isn't an easy project, but it can be worth the effort. When you know your data, you can start to shape priorities around next steps for data security.

Evolving Solutions can help you:

- Get started on a data resilience program starting with DDC.
- Develop a plan for the upkeep, management, and tracking of data.
- Create the ability to classify data in real time or near real time.

IAM: Identity and Access Management

Because every organization has a unique workforce accessing unique resources, identity, and access management (IAM) is unique for every organization.

Evolving Solutions can help you:

- Better understand the role of identity management in improving cyber resilience.
- Take a holistic look at your organization's entire identity system — from mainframe to mobile apps — and walk you through the journey of internal and external threats to help you understand how systems can be misused.
- Develop the processes to effectively manage identities throughout their entire life cycle, including the role identities play in incident response.

EDR: Endpoint Detection and Response

You can't protect what you don't know about, so you can't respond to an event on an endpoint you don't know about. Without comprehensive endpoint visibility, you're leaving the front door open.

Evolving Solutions can help you:

- Get a holistic view of your endpoint security strategy and tactics.
- Recommend and implement solutions based on your business needs, such as CAASM and Microsoft Intune and Autopilot.

Network Resilience

Evolving Solutions has been having discussions about network architecture and design for many years. We've seen what works, what doesn't work, and what makes sense in a Modern Operations environment where business transformation is key to organizational success.

Evolving Solutions can help you:

- Run workshops to help you understand how to secure the different components of a modern network and what your organization should consider based on your environment and business goals.
- Update your network design and implement technologies that will improve network resilience while helping you meet your objectives for network performance.
- Understand if network detection and response (NDR) or secure access service edge (SASE) are a good fit for your environment.

ASM: Attack Surface Management

Most organizations prefer to get started with ASM by evaluating their external attack surface. We can help you get up to speed with that, and from there, work to understand your on-premises and cloud footprints, along with your remote workforce, to guide you in next steps for getting the most value from an ASM solution.

Evolving Solutions can help you:

- Determine whether ASM can address your vulnerability issues.
- Develop requirements around ASM and select the right vendor and tool based on your needs and requirements.

SOAR: Security Orchestration, Automation, and Response

The key to cyber resilience success is automation — the ability to contain a threat without waiting for human input. Automating incident response with SOAR can make a substantial difference in the speed and effectiveness of your response capabilities.

Evolving Solutions can help you:

- Select the SOAR solution that best meets your needs.
- Define and refine processes and build the playbooks that SOAR will automate.
- Ensure that your processes don't miss any steps so that automations will have real value.
- Hit the ground running with SOAR so it can deliver on its promise of immediate containment in the event of a security incident.

XDR/MDR: Extended Detection and Response — Managed Detection and Response

XDR and MDR compress incident response times to help contain an attack before it becomes a business problem.

Evolving Solutions can help you:

- Sort out the many options for XDR.
- Ensure the right integrations are in place to make your XDR investment work for you.
- Recommend one of several companies that provide MDR services and help you investigate the best fit based on your environment and security goals.

Developing a Cyber Resilience Strategy

Developing a cyber resilience strategy can be a big project, so it's not uncommon for organizations to reach out for help. Evolving Solutions has a strategic view of technology and how it supports business operations.

Evolving Solutions can walk you through each step of the strategy development process, including:

- Defining the technology requirements for specific business functions.
- Prioritizing recovery steps.
- Matching the right people, tools, and processes to a recovery plan.

In addition, Evolving Solutions can help you:

- Identify gaps in tools, processes, and responsibilities.
- Develop the tabletop tests and physical tests needed to validate a strategy and help you with the periodic assessments.
- Create a strategic cyber resilience plan that will minimize disruption if the worst happens.
- Ensure that your technical investments in resilience will deliver value in the event of an incident.

12. WORKING WITH EVOLVING SOLUTIONS

PEOPLE SIMPLIFYING TECHNOLOGY

Evolving Solutions brings together industry expertise with real-world experience with organizations of all sizes and complexities. This gives us a unique understanding of our clients' challenges and the outcomes they want to achieve.

Our holistic approach ensures our clients establish a strong and resilient security posture to protect their organization.

ABOUT EVOLVING SOLUTIONS

Evolving Solutions helps clients modernize and automate mission-critical applications and infrastructure to support business transformation. We provide consulting services and technical solutions to enable Modern Operations in a hybrid cloud world.

www.evolvingsol.com/security

EVOLVING SOLUTIONS

Let us help you get started down the right path to Cyber Resilience.

Let's get to work!