The Security Playbook for Remote-first Organizations

nightfall.ai/security-playbook-for-remote-first-organizations

January 28, 2022

The sudden shift to remote work in 2020 exposed companies to a variety of new security challenges that haven't gone away. Review the seven most crucial areas of security for emerging remote-first organizations. Continue reading below or feel free to download a copy of this playbook. We'll also include our free Post-COVID Security Checklist as a reference you can keep in your back pocket.

2020 introduced a permanent change to the security landscape: long-term remote work. As we enter what might be the final phase of the COVID-19 pandemic, we thought it would make sense to review how organizations can strengthen their remote security programs. This article is intended to provide a high-level overview of the critical processes and controls security teams should implement across their organization to compensate for the move to remote work. We've identified eight key security areas that companies should focus on to simplify managing their remote workforce.

Who is our Remote Security Playbook for?

This Remote Security Playbook provides a comprehensive look at security practices, controls, and procedures that are meant to apply to organizations of all sizes. Although this playbook details security terminology and technologies, discussion of these topics will be kept high level so that both technical and non-technical individuals can follow along. The purpose of this playbook will be to provide an overview of emerging areas of focus for organizations within the past year. While not every topic we cover will apply to every single organization, the intent is for readers to evaluate the areas that apply to their organization regardless of their role. If you're a business leader, for example, you can leverage this

playbook to initiate a discussion between yourself and your organization's security team to ensure that they're doing enough to maintain a healthy security posture. If you're a security practitioner, you can use this playbook to improve or validate your organization's best practices.

How did we structure our Remote Security Playbook?

Our Remote Security Playbook is organized into seven core security areas across three categories: people, process, technology. These three categories constitute what is known as the PPT framework. This framework is one crucial way that business leaders, business managers, and security practitioners have evaluated the effects of organizational changes. Security has always required organization-wide support. Thinking about security solely in terms of what the security team is able to do limits the effectiveness of security policies and technologies. To that end, we leveraged the people, process, and technology framework to provide a holistic and layered approach to security.

We validated our seven security areas by referencing the National Institute of Standards and Technology Special Publication series (commonly known as NIST SP 800). NIST is a part of the U.S. Department of Commerce and has helped create science and technology standards that are used across multiple industries. Although there are many great cybersecurity frameworks—NIST even has a second, more high-level framework known as NIST CSF—we choose to focus on NIST SP 800 because of its granularity and level of detail. Both NIST frameworks are a gold standard and are robust enough to apply to any organization, regardless of size or industry.

Throughout our Playbook, we'll reference sections of the NIST SP 800 series that will elaborate on how you may evaluate or implement a specific technology or process.

Section A: Employee Security Awareness

In this section, we'll be focusing on the "people" section of the PPT framework. We'll guide you through the ins and outs of building and maintaining a world-class employee security awareness training program in the post-COVID era.

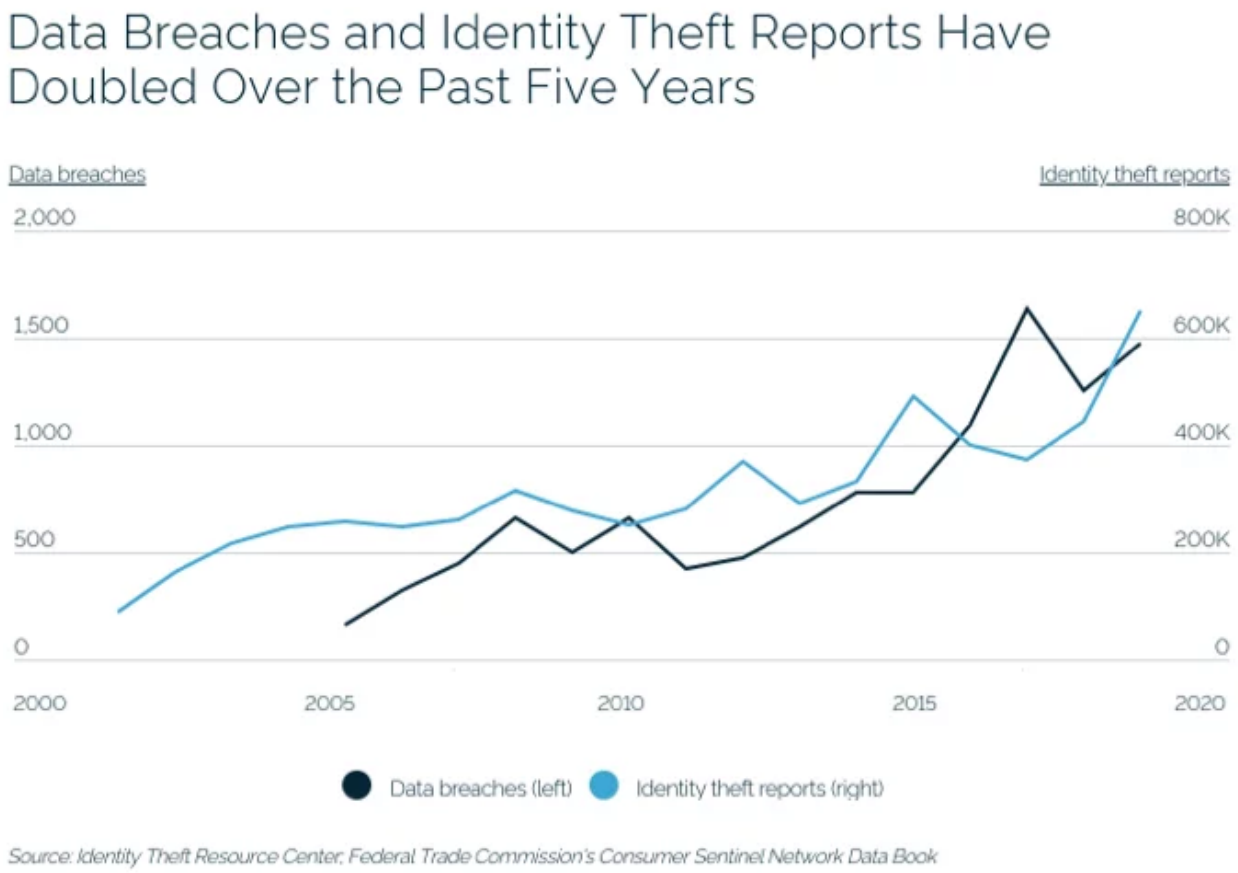
What is the role of security awareness training?

Did you know that every 39 seconds a hacker attempts to break into a system? That's why it's never been more important for organizations to ensure they harden their first line of defense — their employees. The constant barrage of cyberattacks perpetrated by online criminals means that it's a matter of time before hackers attack your organization by targeting employees and contractors. A good cybersecurity awareness training program prepares employees and even contractors for an eventual encounter with hackers by educating them about the telltale signs of a cyberattack, as well as how to maintain good security hygiene and appropriate security best practices based on their role within the organization.

Why employee security awareness training matters in 2021

2020 was a watershed moment for both security teams and organizations as a whole. The shift to remote work changed the way employees worked and communicated with one another. As the workforce moved from cubicle to home office, the devices, networks, and programs used for work changed. Consider, for example, that after the shift to remote work, Malwarebytes, Morphsec, and IBM all found that over half of remote employees used personal devices for work-related tasks. This means that threats targeting these devices could jeopardize corporate data. Companies must now grapple with corporate cybercrime targeting company-owned systems, as well as consumer cybercrime targeting their workforce's personal devices.

In addition to these changes, we've seen an astronomical increase in social engineering-related cybercrimes. These are attacks leveraging email, text messaging, social media, and other forms of everyday electronic communication platforms to scam employees into providing hackers with important information that can help break corporate systems or steal data from them. More specifically, phishing attacks and ransomware attacks have seen gargantuan increases in the past year. By some estimates, ransomware is up more than 1000% in key industries like banking, and phishing campaigns are up over 200%. This trend isn't reversing, as estimates suggest that ransomware attacks now happen as frequently as every 11 seconds. Employee security awareness training can help organizations ensure that their workforce can properly navigate these changes to the security landscape by internalizing the organization's best practices and up-to-date knowledge about today's security threats.



According to the Identity Theft Resource Center from 2005 to 2019 the number of records exposed in data breaches increased over 600% while the number of breach incidents increased nearly 860%. This corresponds to a proportional growth in cybercrime.

How do you build an employee security awareness training program?

While the specifics of an organization's employee security awareness training program will vary based on the industry and practices unique to it, there are two key aspects of a security awareness training program: security policy knowledge and security hygiene knowledge. Security policies are the actual policies your organization will implement as standards of your business. For example, if your organization operates in an industry where personally identifiable information (PII) is regulated, and this information must be shared between specific employees for work purposes, you might have a data confidentiality policy outlining for employees that handle this PII when, where, and how they can share it. Security hygiene knowledge refers to more general information security knowledge that will keep employees safe, like not reusing the same password across multiple services, recognizing the signs of a social engineering attack, and other related practices. A good information security program will educate employees on the policies that are relevant to them based on their role and ensure that they demonstrate competency about basic aspects of security hygiene.

Five steps for developing a world-class employee security awareness training program

There are five important steps for ensuring that your workforce develops the perfect balance of security policy knowledge and security hygiene knowledge. We've discussed some of these before in a blog post focused on building a culture of security among remote employees, but will further elaborate on them below.

1. Show you're serious by developing a culture of security awareness

The most critical aspect of developing a security awareness training program is building a culture of security within your organization. While your security awareness program will undoubtedly be the core of your organization's culture of security awareness, without critical infrastructure supporting this program it's doomed to fail. At the bedrock of this culture should be organizational policies that inform the behavior of everyone within your organization, from entry-level employees to executives. This process starts with organizational leadership working with relevant security and technology stakeholders to translate your organization's ethos and security goals into security policies that ensure your employees maintain the highest standard of conduct while working for your organization. These policies will be the foundation with which you will actually build your security awareness program. If you're looking for inspiration for building robust security policies, the SANS Institute, an information security training and certification resource, provides a variety of security policy templates that illustrate the types of security policies your organization might choose to adopt.

2. Build a comprehensive security awareness training resource library

In order to help employees keep their knowledge of security policies and security hygiene top of mind, building a security resource center that will store important security lessons as well as abridged versions of important policies will be extremely useful. This library will serve as a reference for employees and will be critical in bolstering a culture of security awareness among your organization's workforce. The good news is that even if your organization lacks lessons or exercises of its own, a library can be created from a blend of internal and external content. Groups like the National Cybersecurity Alliance and others provide resources like security awareness training quizzes and tools. Additionally, security awareness training platforms could provide this service for your organization.

3. Provide role-based security training

While all employees can benefit from having a thorough understanding of security hygiene and the values that inform an organization's security policies, individuals in specific roles with access to highly sensitive information might require training unique to them. This training should likely complement any training centered on processes and technologies unique to their role as well. NIST Special publication 800-53 provides an overview of which considerations might be relevant when developing role-based security training. Some of these include frequency as well as whether the role involves managing environmental, physical, or security controls.

4. Test and benchmark employee security awareness training

To develop a truly robust security awareness program, benchmarking and tracking the progress of your employees matters. Most organizations often do this with periodic quizzes or even simulations, like fake phishing emails created internally and sent straight to employees' inboxes. Whether your security awareness team creates its own security exercises or uses a security awareness or phishing simulation platform, the idea is to validate that employees are developing a detailed understanding of security hygiene and internalizing security policies. Since the ultimate goal is to leverage your employees as resources that can potentially identify cyberattacks in progress, employees and departments that are successful in identifying real or simulated incidents should be recognized for doing so during performance reviews and evaluations.

5. Have someone own security awareness within the organization

Because security awareness training programs are a critical part of maintaining an organization's security posture, it makes sense to have someone who helps implement and maintain the program. This person could be a security practitioner or a business manager, so long as they have an understanding of the organization's policies as well as what security metrics make sense for the organization so that they measure employee performance within the security awareness training program effectively.

Section B: Security Controls

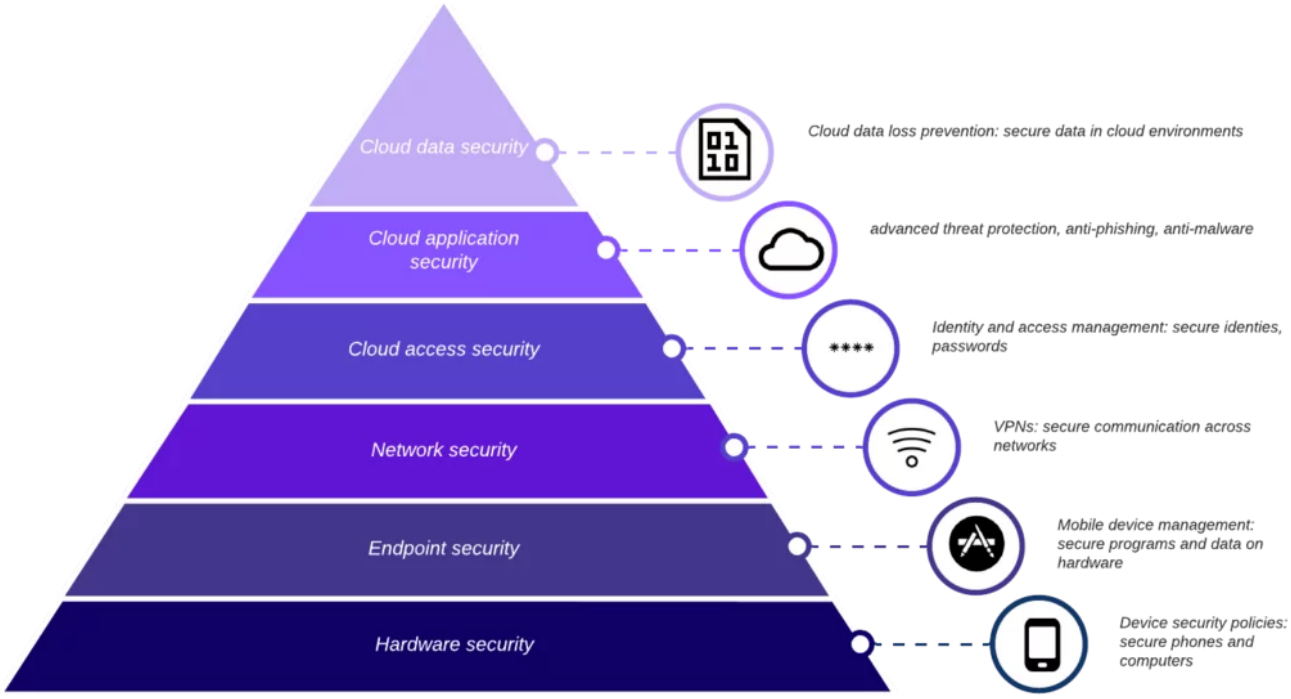
In this second section, we'll be providing an overview of four important security controls that might be relevant to your organization. As you read section B, keep in mind what technologies are integral to your workforce's day-to-day operations so you can prioritize which controls would be most relevant to your organization's security.

What role do security controls play in your information security program?

Security controls are what enable organizations to realize their security policies by allowing security teams to prevent, detect, or correct a security irregularity. While there are dozens of security controls that both individuals and organizations can choose from, in this section, we're going to focus on four controls. These specific controls were chosen because they each protect data at different layers of security.

As a data security company, we promote a security approach called Defense in Depth (sometimes abbreviated as DiD), which means that your security controls should be deployed in such a way that if one fails another can take its place. You can think of defense in depth like the layers of an onion. As an intruder attempts to get deeper into your systems they should continue to meet resistance. Successful information security programs, especially at larger organizations deploy multiple security controls at every security layer, although this can become expensive. Ultimately, however, security isn't simply about having as many controls as possible, but rather about strategically leveraging the controls you have and integrating them with other aspects of your security playbook.

The specifics of what constitutes a security layer for an organization depends on which conceptual model of information security its leaders subscribe to. We're personally fond of the Open System Interconnect model, often simply referred to as the OSI model. We've talked in detail about why the OSI model still matters for information security today, and it forms the basis of our perspective on Defense in Depth security. The OSI model provides an abstract segmentation of computer network communications into seven layers. Data travels back and forth between all layers, starting from layer seven at the top, which is the application layer, all the way down to the physical device at layer one. In our view, the OSI model is simply a reference. Rather than concerning themselves with every OSI layer, modern security teams should identify the technologies used by their organization and map this to a customized version of the OSI model that's more representative of their technology infrastructure. In our post on the OSI model, we briefly detail how some security practitioners have modified the model to make it applicable to cloud infrastructure systems, for example. In the context of remote work security, we imagine something like the following image will be representative of the security layers that will be relevant to most organizations.



Here is a sample view of how your organization's IT infrastructure might map to the OSI model, with the devices employees use at the bottom and the data they access in cloud services at the top.

Let's walk through our sample model to illustrate how you might use something like this to determine which security layers matter for your organization.

An illustration of how Defense in Depth security works

In our hypothetical, we assume an organization's IT infrastructure consists of remote employees using laptops and phones that have access to both corporate intranets as well as popular software as a service (SaaS) applications like Google Drive, Office 365, Dropbox,

and Slack as well as public cloud environments like AWS and Microsoft Azure.

Layer 1: Hardware Security This involves the state of the physical hardware employees will use for work purposes. In an office environment, security often extends to the type of access controls provided by the physical space devices reside in. For example, are laptops supposed to be locked away after work? Do employees need key FOBs to enter the building where laptops are stored? Although remote work has invalidated these particular questions, hardware security remains important. Where should employees use and store work related devices when working remotely? Are they liable for loss, damage, or theft of devices? Your security policies should inform your approach to these questions, and you can use a security control like a mobile device management platform (MDM) or endpoint solution to help keep track of devices and lock them down remotely if they're lost or damaged. We'll cover MDM platforms in the segment below.

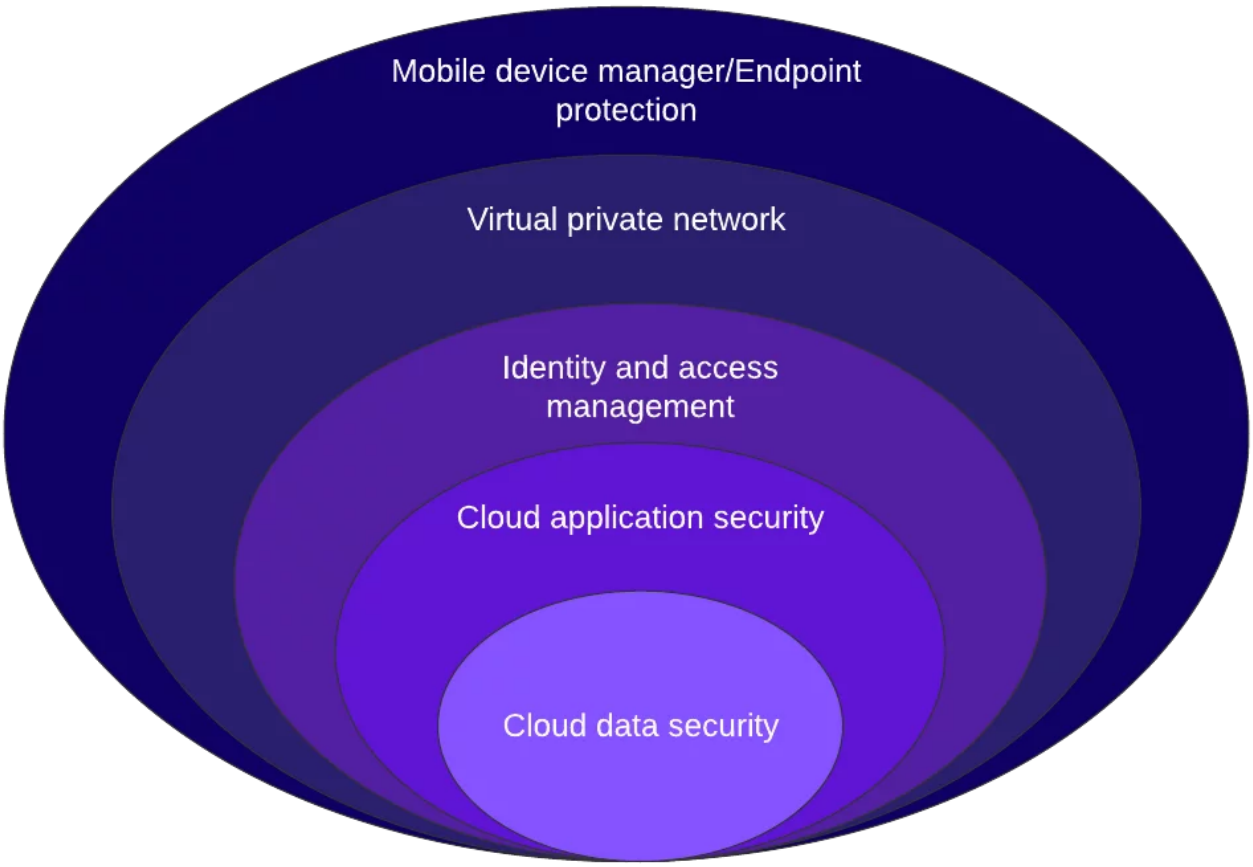
Layer 2: Endpoint Security Endpoint security encompasses some aspects of hardware security, but it also extends to the security of the data and applications running on company hardware or devices that are otherwise used for work. Mobile device managers can also provide security at this layer.

Layer 3: Network Security Network security focuses on securing data moving between employees' devices and corporate networks or to cloud systems. This is usually accomplished with a Virtual Private Network (VPN). We'll be covering VPNs after we discuss MDM.

Layer 4: Cloud Access Security Cloud access security focuses on protecting the passwords and accounts used to access critical systems for work. Identity and access management (IAM) solutions provide security at this layer. IAM solutions will be covered after we discuss VPNs.

Layer 5: Cloud Application Security This refers to securing the actual environments that employees work in. The types of controls you may choose to use at the layer will depend on what types of applications and resources your employees access on a day-to-day basis, but some examples include advanced threat protection, email anti-phishing, and other solutions that focus on preventing or mitigating exposure to malware through applications in the cloud. Since security solutions at this layer are highly dependent on what applications your organization decides to use, we won't be covering them in much greater detail in this playbook.

Layer 6: Cloud Data Security The very last layer involves securing the data stored within the applications and environments that employees use for work. This can be done with cloud data loss prevention (DLP) which we'll cover at the end of section B.



This is a visual representation of how Defense in Depth would work to layer your security with the controls highlighted above.

What is mobile device management (MDM)?

An MDM solution is a security control that allows organizations to keep track of employee devices and manage the configuration of these devices. Historically, MDM solutions predominantly focused on addressing smartphone security; however, MDM security has evolved to include the security of laptops and desktop computers in addition to smartphones. MDM security solutions protect devices in a number of ways, but most commonly they can do several of the following:

- **Data or device encryption**: This feature ensures that data is encrypted at rest. Some services go as far as providing full disk encryption for hardware. This means that if a device is lost or if the hard disk of the device is stolen, the data can't be viewed or modified without an encryption key.
- **Geolocation**: This lets security managers see the location of hardware assets in real time so that they automatically know if a device is being used from a new or unfamiliar location.

- **Geofencing**: Sophisticated MDM solutions might allow security teams to set up geographic boundaries which trigger security features like blocking applications from running if a device is used in an unfamiliar location. Some solutions might also be able to send alerts to a security dashboard based on where a device is being used so that security teams can manually decide how to handle the situation.
- **Remote wiping**: This refers to the ability to delete the contents of a lost or decommissioned device remotely.
- **Mandated password standards**: With this, security teams can enforce specific password criteria when employees create PINs or passwords for their devices.
- **Sanctioned IT**: This refers to the ability to control what applications and resources are allowed to run or be accessed on employee devices and delete applications that break policy.
- **Application sandboxing:** This makes applications run in a container that's isolated from critical system resources and data.
- **Over the air updates**: Centrally manage hardware updates for employee devices.
- **Hardware restrictions**: Prevent specific device hardware from being activated in specific circumstances (microphone, camera).
- **Data partitioning**: Enforce where on a device's hard drive data can be stored. This can be used to separate or "wall off" corporate data from personal data on a device that's used for business and personal use.

Mobile Device Management vs. Enterprise Mobility Management vs. Unified Endpoint Management

While researching MDM platforms you might come across terms like enterprise mobility management (EMM) or unified endpoint management (UEM). While these solutions aren't explicitly within the scope of this playbook, they're worth mentioning because they're intricately related to MDM platforms and provide protection at the device and endpoint layers. There's a lot of confusion differentiating between these solutions, in part because they're very often used interchangeably and have significant overlap with one another. The easiest way to make sense of this is that the term "mobile device management" is the oldest, with "enterprise mobility management" coming afterwards, and "unified endpoint management" being the newest term. The newer terms were coined to reflect an evolution of device and endpoint security, with EMM and UEM encompassing the inclusion of features beyond what MDM platforms historically have offered, like sophisticated sanctioned IT management or integration with anti-malware services. As such, some security companies have taken to calling their offerings EMM or UEM solutions. However, the term MDM not only hasn't been phased out, but still remains the preferred term many companies use to describe their product, even if it includes features offered by EMM and UEM services. This is most likely because as of the time of writing, MDM is still the most recognizable term.

In our analysis, we've included many of the features that these categories shared in common for our comprehensive analysis. Keep in mind, though, that while nearly all EMM and UEM services have MDM functionality, not every single MDM service has the functionality of

services in the other two categories, although many do.

Examples of MDM solutions

Fleetsmith: A solution for SMB/SME organizations focused on securing both iOS and MacOS devices. It was acquired by Apple in mid 2020.

Rippling: An integrated HR & IT platform that has both device management and application management functionality.

Scalefusion: A very popular service that both small and large organizations look to for comprehensive MDM/EMM functionality.

Why are MDM platforms important?

One of the biggest changes that COVID introduced was that it increased the attack surface, or the number of entry points, that hackers could exploit to attack a company's systems or data. This is especially true, not just in terms of the new applications companies are now using—from Slack to Zoom and many others—but as we discussed above, employees are introducing their own personal devices into the equation by using them to connect to corporate networks and work-related cloud services. In our Securing Best of Breed SaaS Applications in 2021 Webinar, we encouraged companies to take a look at how large their attack surface might have grown since the beginning of the COVID-19 pandemic. One of the ways you can do this is using an MDM service to get a handle on the number of devices that are being used for work.

Do you need an MDM solution?

Evaluating whether your organization needs an MDM solution can be difficult, but ultimately comes down to a few considerations, including evaluating your organization's policies, size, and risk tolerance. Below are some considerations that might influence your organization's decision to implement an MDM solution.

1. Where does data live within your organization's IT infrastructure? It's important to understand how your workforce uses your IT infrastructure on a daily basis. For example, if your employees are using applications that run or download data onto their local devices, it's more likely that sensitive data is being stored on their hard drives, which makes the case for using MDM more compelling. Conversely, if your workforce leverages mostly SaaS applications to carry out their jobs, it's more likely that you should prioritize other tools, like cloud DLP, which we'll talk about in a later part of this section.

2. How does IT currently distribute and manage technology assets in your organization? When it comes to deploying MDM and other related security technologies, aside from evaluating where data might live within your organization's IT infrastructure, you'll need to have an understanding of how your IT department intends to manage its assets. Can employees use their own devices for work, often called a "bring your own device"

arrangement, or BYOD, or does the company issue devices? Before you deploy an MDM you'll need to know the answer to this question as it will influence what type of MDM solution you'll purchase because some are better at addressing BYOD risk than others.

What is a VPN?

VPNs are a tried and true technology for allowing remote access to company resources over a secure connection. At the start of the pandemic, in march of 2020, VPN use was estimated to have more than doubled. VPNs provide network layer security by allowing private connections between a device and the services it accesses. VPNs can accomplish this with some of the following features:

- **End-to-end encryption**: VPNs provide encryption or other forms of cryptographic protection for data being transmitted through the VPN.
- **DNS Filtering**: A DNS Filter is a way to block access to specific websites. If you know certain sites are malicious or you simply don't want employees accessing designated sites, some VPNs allow you to filter for these.
- **Kill switch:** If for whatever reason, a device loses its connection to the VPN, the device will disconnect itself from the internet. This is a way to ensure that no unsecure usage occurs.
- **IP allow/deny list:** Some VPNs allow you to have an accepted list of IP addresses that can connect to your organization's VPN or access resources through the VPN, granting greater control over how you can protect your data.
- **Permissions and access policies**: Some VPNs grant granular control, allowing you to tweak what individual users can do and access while using the VPN. This might be a good way of segmenting access to company resources based on an employee's role.

Examples of VPNs

Cisco AnyConnect: A popular VPN among enterprise-sized organizations that is commonly used to securely connect to corporate networks.

Perimeter 81: A VPN for organizations of all sizes that also specializes in Wi-Fi security and secure access to SaaS and IaaS environments.

How do VPNs secure your workforce?

VPNs allow your workforce to access company resources as if they were connecting from your office, protecting your employees, their devices, and most importantly your organization's data from being exposed due to the security limitations that tend to exist in home offices. In order to get the most out of VPN usage, it's important to consider your organization's use case. For example, employees connecting to your organization's intranet and to files stored on your business premises might present different challenges than employees connecting to company resources on public cloud infrastructure. Some solutions

specialize in the latter while others specialize in the former. VPNs are not a silver bullet for network layer security. You should keep the following pieces of advice in mind in order to improve the effectiveness of your VPN deployment:

1. Leverage identity and access management (IAM) to control access to resources while employees are connected through a VPN. We'll talk more about IAM below.

2. If your employees are connecting to a corporate intranet as opposed to a cloud service, **use network segmentation** which divides your network into separate sections to make it harder to jump to systems with critical resources through your VPN.

3. Each employee **should only be connected to need-to-access systems** and not your entire network. As we mentioned above, some VPNs let you set access policies per user or device. You can combine this with an IAM solution and network segmentation of resources for even further security.

4. Patch your VPN software to keep it up-to-date and limit the possibility of exploits being used to access business-critical data.

5. Train employees on how to securely connect to resources remotely through the VPN with detailed remote access policies and training.

6. Additionally, **train employees on avoiding social engineering attempts** designed to steal VPN access credentials.

How do you know if you need a VPN?

Unlike with MDM platforms, which might have a more narrow use case for some organizations, it's very likely that most organizations will find VPNs valuable. Since remote work necessitates that data is transmitted across networks, you'll most likely want a network layer security solution like a VPN. It's worth noting, though, that legacy VPNs are centered around securing access to corporate intranets as opposed to public cloud or SaaS systems, though this is a feature offered by some new and emerging VPN offerings which sometimes go by names like Software Defined Perimeter (SDP). Ultimately, your security policies as well as use case will determine if a VPN makes sense for a part or your entire organization and what type of VPN you should invest in.

What is Identity and Access Management?

Identity and access management or IAM refers to a set of processes and technologies that allow organizations to maintain fundamental information security practices like least privileged access in the cloud, ensuring that right assets receive access to the right resources at the right time. The core objective of IAM systems is to provide one digital identity per individual. Once a digital identity has been established, it must be maintained,

modified and monitored throughout each user's access lifecycle. For reference, see a diagram of the identity lifecycle below. The IAM platforms generally include at least two of the following features:

- **Directory**: Maintains the record of all identities and which systems/resources they have access to. This is absolutely critical in managing each employee's identity lifecycle.
- **User access review and audit logs**: Provides records of user permissions across your org, as well as when and where resources were accessed with user credentials.
- **Single sign-on**: A federated identity management arrangement that allows for authentication across a set of systems/resources with one set of credentials, reducing the need to manage multiple passwords. You've likely encountered this online, as a number of websites now let you sign in with your Google or Facebook accounts.
- **Multi-factor authentication**: This augments the login process by requiring access or knowledge of additional factors besides the account credentials. Two-factor authentication with an email or SMS token is a fairly common form of multi-factor authentication, although in principle there are many things that could serve as a second or even third login factor. It's worth noting that multi-factor authentication can exist as a standalone product independent of IAM.
- **Password manager**: This allows for the creation and management of passwords for multiple accounts. Password management functionality can also exist as a standalone product independent of IAM.

Examples of IAM and IAM Platforms

LastPass for Business: LastPass got its start as a freemium standalone consumer password manager. Over the years, however, it's expanded its offerings. For businesses, LastPass offers comprehensive identity and credentials management.

Microsoft Azure Active Directory: Azure Active directory (sometimes called Azure AD) is Microsoft's cloud-based IAM platform that allows organizations to manage access permissions for both cloud-based systems and corporate networks/intranet.

Okta: Okta is one of the most popular cloud identity management platforms and is renowned for integrating with thousands of cloud and web applications to provide seamless single sign-on functionality.

Why is IAM important?

IAM platforms are critical for enabling organizations to practice two important aspects of information security, the principle of least privilege access and maintaining one digital identity per individual. In effect, this means that the right people have access to exactly what they need to do their jobs; nothing more, nothing less. Additionally, IAM platforms enable teams to quickly provision or alter a user's access to resources based on changes in their needs or employment status. This means that whether someone's promoted or terminated, you can

easily modify or revoke access to the programs, services, and data relevant to them. We'll briefly cover how IAM platforms help you realize all three of these aspects of your organization's security below.

1. Implementing the principle of least privilege with IAM

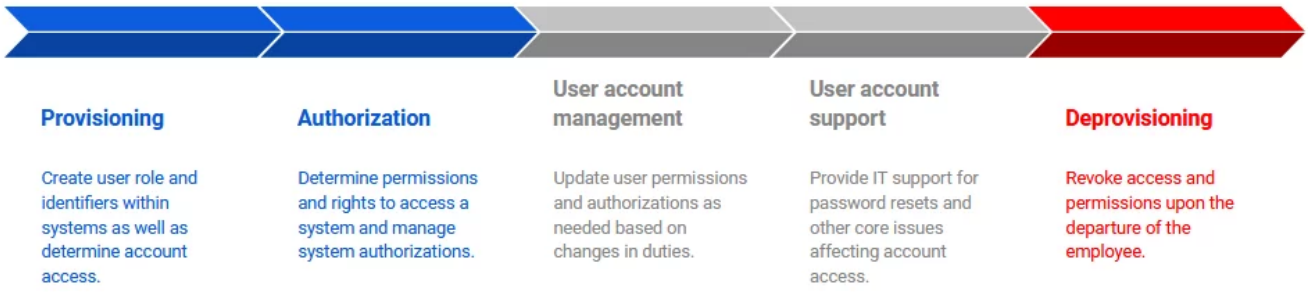
The principle of least privilege access often referred to as just the principle of least privilege or the principle of minimal privilege is a fundamental information security practice that guarantees that any user, process, or program only be given access to the exact resources it needs to complete a task. Providing permissions that grant broader access tends to increase the risk that sensitive data is exposed. Typically, when hackers infiltrate a system, they look for users with the broadest possible access to data and critical systems. Over provisioning access across your workforce simply makes a hacker's job that much easier. In fact, in our 2020 SaaS security risks post we highlighted that 74% of breaches involve abuse of privileged credentials. With IAM platforms, you can manage which users get access to which systems and remove access any time it's needed.

2. Ensuring one identity per individual with IAM

Another fundamental aspect of IAM is to ensure that every individual within your workforce has a consistent identity across your organization. This essentially means maintaining a persistent identity that is tracked and only modified as a result of relevant changes to the person's role or status within the organization. IAM is essential for formalizing the identity lifecycle around business policies specific to your organization, as we've alluded to above. The lifecycle is an important way to illustrate how an employee's access to a system can change over the course of their role. Many IAM platforms let organizations implement policies determining when and how a person's access should change, and these changes can be made on a user by user basis.

3. Managing the identity lifecycle across your workforce with IAM

As we've discussed above, IAM platforms allow for the timely movement of employees to the proper part of the lifecycle based on relevant changes to their role. Without it, accounts that are no longer in use or that have very broad privileges could be used by hackers to view, access, or modify sensitive information. The middle two stages, where IT services these accounts for IAM related requests like helping with password lockouts. New employees are quickly moved through the first two stages, and employees who no longer need access to specific accounts should quickly be moved to the last stage.



A visualization of the identity and access management lifecycle. Keeping track of where each employee is in the lifecycle will help ensure everyone has access to the exact resources they need at the right time.

Do you need an IAM platform?

Many organizations, regardless of their size, will likely find at least one of the features we mentioned above useful. Standalone password managers as well as multi-factor authenticators, for example, can provide a way to create strong and secure passwords while limiting who can access the applications used by your workforce. The good news for sole traders and small businesses is that these standalone products tend to be affordable and very easy to use. The case for more comprehensive IAM functionality, like directories and identity managers, becomes critical for organizations whose policies require they have visibility into employee login behavior. There's also a case to be made for high growth organizations adopting a full IAM suite sooner, rather than later, as the rapid addition of new team members and new applications can easily make identity lifecycle management a security headache and logistical nightmare. Below are two considerations that can make evaluating what type of IAM solution you might need, if any.

1. What does your organization's identity lifecycle look like (and can you deprovision quickly)? One of the first steps you should take in order to validate if your organization would benefit from an IAM platform is to understand your identity lifecycle. Does your organization have policies around provisioning new users appropriate access to the proper resources? How quickly do you deprovision or revoke access to resources that aren't needed anymore? Understanding this will give you a sense of how much risk your current identity lifecycle practices pose to your organization. If your organization is slow to deprovision access, investing in an IAM platform that specializes in directory management or SSO management might help.

2. Does your IT team have a good grasp on which assets require privileged access? Within your organization likely lives data assets that should only be shared on a need to know basis. A second important step is to evaluate where these are with an asset inventory. Depending on where this data lives, you can determine what type of IAM solution makes sense for controlling access to these assets.

What is cloud data loss prevention?

Cloud data loss prevention, or cloud DLP, is an emerging security category that protects against sensitive data leakage within SaaS and cloud infrastructure. Because cloud platforms are always on and often involve collaboration across multiple teams, organizations have found it difficult to maintain or enforce their data security policies at this layer. That's where cloud DLP comes in. Cloud DLP platforms like Nightfall discover, classify, and protect data at this layer with automatic detection and redaction of sensitive data, so that it's only seen on a need-to-know basis. The core features of a cloud DLP platform like Nightfall include:

- **API connectivity:** Cloud security solutions like Nightfall are able to seamlessly integrate into cloud environments in order to scan and secure them.
- **Data discovery:** Within the context of cloud security, data discovery is the ability to provide visibility into the location and attributes of sensitive data, either within files or other contexts. A Cloud DLP platform like Nightfall can find data anywhere within a cloud environment.
- **Data classification:** Within the context of cloud security, data classification is the ability to classify data according to its type, sensitivity, and impact. Nightfall, for example, is able to determine if a piece of data is PII, a credential, or some other sensitive data type.
- **Automated remediation:** A security platform like Nightfall can automatically redact, block, quarantine, or delete incidents of data exposure that violate data security policies.

How does cloud data loss prevention differ from legacy data loss prevention?

Traditionally, data loss prevention, as well as other related technologies such as cloud access security brokers (CASBs), were deployed on an organization's network to monitor traffic leaving the network perimeter. Over the last few years, however, we've seen a shift towards company data originating from within SaaS and cloud infrastructure. This shift was exacerbated by COVID which forced most companies to leverage cloud collaboration tools and infrastructure. As such, these traditional data loss prevention solutions are ill-suited to addressing the data leakage that occurs within the cloud, as they secure data at a different layer. As a pioneer in the data loss prevention space, Nightfall is the first cloud-native data loss prevention solution. This means we're cloud-first and engineered to deploy in SaaS and IaaS platforms literally within minutes. Additionally, our platform leverages machine learning to automate the detection of content that violates predefined security policies, allowing for a highly accurate and modern approach to data security.

Why is cloud data loss prevention so important?

The last decade has been defined by the proliferation of massive amounts of data within cloud applications, systems, and infrastructure. By 2025 the amount of data stored in the cloud by both governments, organizations, and individuals will reach 100 Zettabytes — an estimated 50% of the world's 200 zettabytes of data at that time. Data security within cloud

systems has lagged behind this exponential accumulation of data, which is why solutions like cloud data loss prevention cloud DLP have become extremely important. Cloud DLP provides access controls as well as remediation capabilities for incidents violating data policy, like improper sharing of sensitive data. Such incidents are likely to be more common in a work from home environment and will be hard to detect unless you're explicitly watching for them. Organizations will likely find that as their usage of cloud services grows, they'll need a solution like Nightfall to mitigate data exposure risk and ensure compliance with a growing number of data privacy regimes.

Section C: Security Processes

In this section, we'll be looking at important security processes that you'll need to implement and develop as your remote workforce grows.

What role do security processes play in your information security program?

Security processes are the third critical pillar of your organization's information security program. Having well-defined security processes in place before your organization experiences a major security incident is important, given that effective processes will help teams navigate how to appropriately respond to security incidents. For this section, we've specifically focused on a handful of processes that are critical to returning your organization back to normal once a business disruption occurs: business continuity and remote incident response. We'll also very briefly discuss other areas of focus that apply to some organizations, like vulnerability management and third-party risk.

What's the difference between security policies and security procedures?

Throughout this playbook, we've used the term security policies to describe the rules or guidelines that should inform both employee behavior and the configuration of your security controls. You might be wondering how this is distinct from the security processes we're talking about in this section. The critical difference is that policies articulate the behaviors that allow for normal operation within your organization, whereas procedures are actions explicitly taken by IT or security stakeholders in order to respond to incidents or potential incidents. Both are central to your information security program.

What is business continuity?

Business continuity refers to the ability for organizations to continue working after a major disruption. Organizations use business continuity plans to establish which processes and technologies are essential for operating the business. Business continuity planning is often paired with a disaster recovery plan, which ultimately will allow an organization to return to operating under normal conditions. Business continuity has been a growing concern post-COVID, as the pandemic has taught many organizations the risks of not having a business continuity plan before a major disruptive event like COVID. The pandemic has also revealed

that business continuity plans also need to be robust enough to accommodate multiple simultaneous disruptions, as some organizations had to deal with COVID-19 and natural disasters simultaneously.

How to create a business continuity plan

A business continuity plan is a cross-functional document that requires the coordination of multiple stakeholders across an organization. While some of its contents might be outside the purview of IT and security teams, it's important to involve these groups when building the plan so that they understand what their role is in supporting the organization during a disaster, and so that they can provide input regarding which technologies and security policies can be supported during that time. Business continuity planning is a process that requires multiple steps. While ultimately no two organizations will rely on the exact same process or plan, we've outlined essential steps to consider if you need help getting started with the process.

1. Create a business continuity team by identifying relevant stakeholders

Knowledge of a business continuity plan isn't something that every single employee needs to have, nor a process they need to be involved in. Before work on such a plan can begin, organizational leaders should come together and identify the individuals who need to be involved in the process. This selection process will ultimately be unique to each organization carrying out this task, but as we suggested, given the role technology and security teams will likely play in enabling business continuity and disaster recovery, having IT and security stakeholders will be critical.

2. Conduct a business impact analysis

In tandem with understanding which stakeholders should be informed or directly involved in the business continuity planning process, it's important to also understand the risks posed by disruptions. This is often conducted through a business impact analysis (BIA). The primary focus of the BIA is to measure the immediate costs and duration of a business disruption. The BIA should also assess what processes and resources the organization needs at the bare minimum to function, especially if this is the first BIA your organization has ever conducted. Securing these critical resources during a crisis will be essential to the organization's survival. Should this assessment identify gaps in the organization's ability to carry out essential procedures and provide access to essential resources during a disaster, a separate plan should be developed to articulate how this will be rectified.

3. Develop the business continuity plan

After establishing the team responsible for managing your organization's business continuity plan and determining the processes and resources that need to be in place during a crisis, the work to create and implement a business continuity plan begins. A business continuity plan should begin by defining the goal and scope of the plan. For example, your BIA might reveal that the costs of a specific type of disruption are unacceptably high, and so your stated goal could be to reduce costs incurred from the disaster. For another organization, the

goal could simply be to maintain uptime for company resources for employees or customers. You'll also want to consider creating plans for multiple types of disruptions. It's likely that your organization will be impacted by a cyberattack differently than a disaster that prevents access to your office and the physical assets within. Some common contingencies that your organization might wish to prepare for include pandemics, natural disasters, cyberattacks, power outages and/or downtime of critical technology services like payroll or payments processing.

4. Validate your business continuity plan with a tabletop exercise

Your business continuity plan does no one any good if it's not realistic or applicable in the event of an actual crisis. One of the ways companies validate their plans is to engage in tabletop exercises. Tabletops are meant to be walkthroughs of specific scenarios for your entire organization. During your tabletop exercise, you can pull in leadership, as well as the staff who will be involved in executing parts of the business continuity plan. You'll have everyone review and go over their roles in relation to whatever scenario you've decided to base the tabletop on.

What's the difference between business continuity and disaster recovery?

As we alluded to above, business continuity plans tend to detail your immediate response to problems caused by a disaster, and often the goal is to simply contain these issues and get the organization operating in whatever capacity possible. Business continuity planning also evaluates the impact of the crisis in terms of broader business goals and resources. Disaster recovery is a process that more narrowly focuses on the IT resources needed to sustain the business after a crisis and ultimately return operations to normal. This, of course, is a process that heavily involves IT and security stakeholders. When it comes to the role of such stakeholders in business continuity planning, they should help identify critical systems that will enable operations while developing full IT disaster recovery plans that will be appended to your organization's business continuity plans.

What should be included in a disaster recovery plan?

NIST SP 800-34 provides a highly detailed analysis of what IT and security teams should consider when developing a disaster recovery plan as part of business continuity plans. NIST recommends a seven step plan in order to help organizations build out their disaster recovery plan (referred to as the Information System Contingency Planning Process). The seven steps in the process are:

1. Develop the contingency planning policy. Contingency planning policies state the focus of a given disaster recovery plan, which is generally to support the business continuity plan it supports. This requires articulating which IT assets and resources are essential for supporting the organization

2. Conduct the business impact analysis (BIA). As part of the BIA conducted for the business continuity plan, IT stakeholders should include assessments of what will happen if key IT systems or infrastructure fails, including which employees or customers will be affected and which business processes will be affected. You can use this analysis to determine how much money and time disruption of IT assets will cost the business and how much it'll cost to repair. With this assessment you should be able to determine what amount of downtime of assets will be acceptable for the organization.

3. Identify preventive controls. In tandem with the BIA, IT stakeholders should identify controls that can help reduce the likelihood of IT infrastructure failure and develop a plan for implementing and monitoring these controls.

4. Create contingency strategies. NIST SP-800 34 highlights the need for contingency strategies for maintaining special resources like backup and recovery capabilities, offsite data storage access, and the ability to replace damaged equipment.

5. Develop an information system contingency plan. This step involves using the results from the previous steps to develop your IT disaster recovery plan.

6. Ensure plan testing, training, and exercises. After developing your plan, you'll want to test its viability. This should be done in combination with testing your overall business continuity plan and IT and security stakeholders should be involved in any tabletops relevant to those plans. Additionally, though, IT and security teams will need to also test the disaster recovery plan. Outside of tabletops, these teams should run through actual simulations of disaster events where team members perform their assigned roles.

7. Ensure plan maintenance. Even when the plan is not in use, it needs to be kept up-to-date to ensure that it's ready to be used wherever disaster strikes. Organizations should review both their business continuity and disaster recovery plans at regular intervals and ensure that testing and training exercises are using the most up-to-date plans.

What is remote incident response?

Incident response is closely related to business continuity and disaster recovery. It is effectively how your security and IT teams will respond to a technology or cybersecurity related disaster that may or may not result in organization-wide disruption. For this reason, Incident response plans should be created in sync with disaster recovery plans and informed by any security and technology related weaknesses highlighted in your BIA. While building incident response plans and policies are among standard information security best practices, many security teams will likely need to revisit these post-COVID and adapt them to the demands of a remote-first world. This involves understanding the nature of remote security incidents, as well as understanding the composition of remote security teams and the means

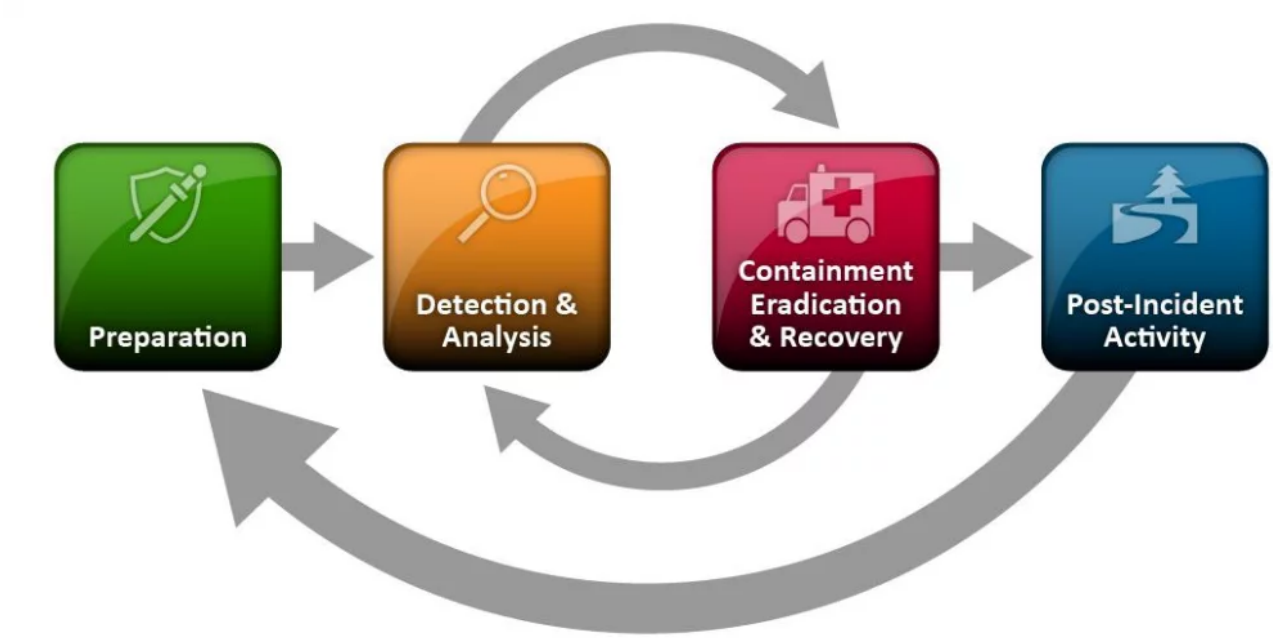
by which these teams will discover incidents and communicate with one another. Below, we'll briefly cover some important steps to consider as your organization builds out its incident response capabilities.

1. Identify remote security risks

Having an understanding of the types of security threats your organization faces is going to be critical in building your capacity to respond to them. In addition to the threats identified through a BIA, incident response policies should be tailored to the remote risks identified through audits, logs, and employee security awareness programs. Security teams should regularly assess risks by reviewing these and developing strategies to respond to incidents stemming from these risks.

2. Develop an incident response lifecycle

Frameworks like NIST provide a way to map the various steps of the incident response process to phases that correspond to the age of an incident. This is called the incident response lifecycle. Much like the identity lifecycle, this is a way for teams to easily keep in mind what steps they should focus on taking as the incident progresses. Below we've posted the incident response lifecycle as it appears in NIST SP 800-61. It will likely make sense for security and IT teams in your organization to validate if these phases make sense and determine what processes correspond to the phases of the cycle.



3. Create an incident response plan

Just like with business continuity and disaster recovery, a successful implementation of incident response capabilities will hinge on having a plan. This incident response plan, like the plans discussed above, should have a defined goal and scope. NIST SP 800-61 outlines the following steps for establishing an incident response program within your organization:

- Create an incident response policy
- Develop procedures for performing incident handling and reporting
- Set guidelines for communicating with outside parties regarding incidents
- Select a team structure and staffing model
- Establish relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department)and external (e.g., law enforcement agencies)
- Determine which services the incident response team should provide
- Staff and train the incident response team

What are other security processes you should consider?

Before we conclude, we wanted to briefly mention other security processes that might make sense for your organization to evaluate depending on size and industry: Vulnerability management and third-party risk.

What is vulnerability management?

Vulnerability management is the process of identifying, prioritizing, and remediating vulnerabilities within IT resources, assets, and applications. Vulnerabilities (especially zero-days) represent one of the most critical security threats organizations face, and vulnerability management is one way to assess risk in this area. Vulnerability management begins with developing an inventory of assets in order to track relevant updates and patches for them. The development of an asset inventory should be combined with continuous visibility of the settings and configurations of these assets. Some of the security controls we've discussed above, like mobile device management solutions, can help you inventory and remediate device vulnerabilities by letting you push updates to devices over the air. You might require something more sophisticated, however, for custom applications or for applications that your organization has personally created.

What is third party risk management?

For a number of organizations, securing their business isn't simply a matter of deploying controls and processes within their own environments; they also have business partners who have access to critical data. In this case, it's important for organizations to conduct a third-party risk assessment to determine the ways in which partner relationships could result in reputational harm, supply chain disruption, and security incidents or business continuity failures. If a third party is pivotal to essential functions in your organization, you've likely identified some of these risks in a BIA. If not, you can begin a third party risk management process with a plan similar to the ones we've recommended above and leverage popular risk management frameworks to determine best practices for maintaining a third party risk management program.

Putting it all together

We've covered a lot of ground in this post. Using the People, Process, Technology framework we identified strategic security areas across these three different organizational categories. We looked at the hows and whys of this framework, and the way in which policies and education of employees is reinforced by proper security controls and security processes carried out by your security team. We also explained what it is many remote organizations are ultimately defending—sensitive data that moves from employee devices and ultimately ends up in the cloud. Using the OSI model as a reference, we highlighted a layered approach to security controls that provide Defense in Depth. Finally, we looked at security processes as a way to address what to do when things out of the ordinary, like business disruptions and security incidents, occur.

Because we covered so much in this post, it makes sense to again highlight how you can get the most out of the document. One of the first things we recommend is to identify stakeholders within your organization to whom details of this playbook apply to or otherwise resonate with. While this is ultimately a security playbook, we've made no assumptions about you as a reader. If you're a business manager or a non-IT leader, it might make sense for you to have a cross-organizational discussion with security leadership. If your organization doesn't have this function, you can approach business leadership instead. Conversely, security practitioners and leadership can use this playbook to validate their existing strategies and possibly discover new ones. We're also hopeful that small businesses can strategically pick out aspects of this playbook that apply to them. Keep in mind that you don't need to implement the entirety of this playbook at once, and it might make strategic sense to only focus on one section or individual item at a time. It will also make sense to identify which policies, processes, and controls you already have in place or which ones otherwise might not apply to your organization.

While this playbook contains a variety of practices and technologies, it'll ultimately be up to you to determine what makes sense for your organization to implement. If it's the case, for example, that much of your sensitive data lies within internal corporate or enterprise networks, then an emphasis on anti-phishing training, VPN security, and vulnerability management make sense. If your asset inventory suggests that employees have rapidly adopted new cloud collaboration tools, possibly ahead of your organization's ability to secure these environments, then leveraging cloud data loss prevention for data discovery, classification, and data exposure remediation would be far more critical to your security strategy. With that said, we hope this playbook as well as the accompanying checklist serve as a point of discussion between both business leadership and security stakeholders. Our ultimate goal is to help organizations get a handle on where business-critical data travels and lives. We're confident that using this playbook and working side-by-side with key leaders will ensure that your organization successfully adopts to the new era of remote work.

Resources

The resources here are meant to provide you with additional reading on topics brought up in the playbook.

Should Failing Phish Test Be a Fireable Offense – An article that covers why positive reinforcement is ultimately best for security awareness programs.

NIST SP 800-50 Building an Information Technology Security Awareness and Training Program

NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise

NIST SP 800-63 Digital Identity Guidelines

Choosing a DLP Solution: A Guided Plan

Cloud-native as the future of data loss prevention

More on business preparedness exercises

The Post-COVID Security Checklist for Remote-First Organizations

Section A - Employee Development

1. Employee handbook and security education

- [ ] **Use employee handbooks to summarize complex security policies.**

  Organizations should include high level summaries of key aspects of their email, equipment, password, remote access, and acceptable use policies within their employee documentation.

- [ ] **Personalize security education.**

  Tailor security education based on the level of access of an individual employee, in addition to conducting more general cybersecurity training that discusses the tools, best practices, and risks unique to your org.

- [ ] **Measure security awareness within your organization.**

  Use measurable objectives to validate the success of cybersecurity education. You can utilize exercises like phishing drills to track employees' security awareness over time.

- [ ] **Allow employees to reference security lessons on-demand.**

  Employees should also be provided with access to a security library where they can view all security policies and relevant security training.

Section B - Security Controls

2. Mobile Device Management (MDM)

- [ ] **Consider what working arrangement will be best for your organization.**

  Can your employees use their own devices (BYOD) or do you want to have more control by issuing company-managed devices? This decision should be made before you commit to a strategy for securing assets.

- [ ] **Determine what user behaviors are acceptable on devices used for work.**

  MDM secures devices used for work, which is why it's important to develop an acceptable use policy to inform employee behavior. For example, if your org issues devices to employees, you might choose to only allow sanctioned applications to run on these devices and use a MDM to enforce this policy. Conversely with a BYOD scheme, you might have employees install a MDM that lets apps "for work" run in a sandbox on employees' devices.

3. Virtual Private Network (VPN)

- [ ] **Combine VPNs with network and application layer security options like access controls.**

  Leverage identity and access management tools to control how to access data and systems when employees connect to corporate networks over VPN.

- [ ] **Keep your VPN up-to-date.**

  Patch your VPN software to keep it up-to-date and limit the possibility of exploits being used to access business-critical data.

- [ ] **Use phishing drills and exercises to help employees recognize attempts to hijack their VPN credentials.**

  Additionally, train employees on avoiding social engineering attempts designed to steal VPN access credentials.

- [ ] **Ensure that sensitive data and resources remain on a "need to use" basis over VPN.**

  Use network segmentation and identity and access controls to make it harder to jump to systems with critical resources through your VPN. Each employee should only be connected to need-to-access systems and not your entire network.

- [ ] **Ensure employees understand how to log into your VPN securely.**

  Train employees on how to securely connect to resources remotely through the VPN with detailed remote access policies and training.

The Post-COVID Security Checklist for Remote-First Organizations

4. Identity and access management (IAM)

- [ ] **Build an asset inventory to determine which resources require privileged access.**

  Evaluate your security policies to identify tools, software, and systems that require additional forms of security like identity or privileged access management.

- [ ] **Prove the value of identity lifecycle processes.**

  Utilize access and incident management logs to keep track of identity-based security risks as well as to validate the effectiveness of your identity management processes.

- [ ] **Formalize your organization's identity lifecycle.**

  Leveraging your asset inventory, identify the tools and services employees will need upon provisioning based on their department and role and develop a consistent process for deprovisioning resources when they're no longer needed or when users leave the org.

5. Cloud data loss prevention (Cloud DLP)

- [ ] **Conduct an audit of your data assets.**

  The key to effectively using cloud DLP is to understand which cloud systems pose the greatest data exposure risks. Determining what SaaS and IaaS applications are in use within your org, who maintains them, and what they're used for can help evaluate if you need the visibility and security controls cloud DLP provides.

- [ ] **Use data-centric security policies to automate your cloud security.**

  Leveraging cloud DLP requires you to have an understanding of the types of data security requirements you need to adopt to maintain a healthy security posture. What combination of PII and sensitive data would count as data exposure? A product like the Nightfall DLP policy engine can help you translate your answer into rules that automate data loss prevention.

Section C - Security Processes

6. Business continuity & resource management

- [ ] **Harden existing continuity plans by prepping for multiple simultaneous business disruptions.**

  As 2020 has proven, it's possible for an ongoing disruption, like a pandemic, to coincide with other types of disruptions like extreme weather events. A resilient business continuity plan must detail how to continue operations under multiple disruptions.

- [ ] **Evaluate service level agreements with third-parties to determine if vendors meet uptime requirements.**

  In addition to benchmarking and maintaining uptime standards within your own org, you should determine if vendors and other third-parties whose services you rely on meet your uptime standards in light of the move to remote work.

- [ ] **Build out systems for tracking uptime and guaranteeing continuous availability of core resources.**

  In tandem with incident response policies and business continuity plans, organizations need to benchmark resource uptime and incorporate remediative processes for events that disrupt uptime into both of these.

7. Remote incident response policies

- [ ] **Tailor incident response strategies to remote risks.**

  Leverage identity and access management logs, employee security awareness benchmarks and learnings from recent audits or asset inventories to identify risks currently faced by your org.

- [ ] **Evaluate the composition of incident response teams in light of remote work.**

  With entire organizations remote, security leaders will need to have a good handle on how incident response teams are composed and devise effective processes for teams to discover and communicate incidents to one another and the org at large.

8. Vulnerability management

- [ ] **Maintain a living inventory of asset settings.**

  Vulnerabilities (especially zero-days) represent one of the most critical security threats organizations face. The development of an asset inventory should be combined with continuous visibility for the settings and configurations of your org's assets.