THE COMPLETE GUIDE TO THE NIST CYBERSECURITY FRAMEWORK

UPDATED FOR 2023

From CISOs to SecOps teams, find out how the NIST Cybersecurity Framework is evolving and what you should be doing to achieve and maintain a compliant cybersecurity posture.

Lepide

CONTENTS

INTRODUCTION

In the US, there isn't a single data security law for the private sector. Instead, there are separate data laws, principally HIPAA and GLBA, covering their respective sectors of health and finance. However, there is a legislative effort underway in Congress, the American Data Privacy and Protection Act (ADPPA), to provide uniform privacy and security rules of the road . It may eventually become law, but it still has a few significant barriers to overcome.

This doesn't mean that the US government has nothing to say about what a good data security program should look like. In fact, just the opposite is true. The US has offered significant guidance to the private sector on security issues. In 2014, President Obama announced the launch of the Cybersecurity Framework (CSF), which is a voluntary program for companies to improve their cyber readiness. For its part, the National Institute of Standards and Technology (NIST) released version 1.0 of CSF, which provided a kind of super standard that would incorporate “existing global standards and practices”. It organized many common data security standards into five functional areas — the now familiar Identify-Protect-Detect-Respond-Recover model.

While initially intended for companies in the critical infrastructure space (of telecom, banking, transportation, and energy), CSF’s powerful model has since gained popularity and is now accepted as a worldwide standard. It continues to evolve, and there is an effort underway to complete version 2.0 of the Framework.

What makes CSF so popular?

There are a few key benefits. First and most importantly, CSF allows IT groups to follow their existing security standards — say ISO 27001 or PCI DSS — and still maintain compliance to them. That’s because CSF is more like a meta standard.

This leads to the second benefit. CSF organizes security controls into the five functional groups mentioned above. CSF lets you view separate controls — there can be hundreds in a standard — as part of higher-level groupings. Rather than thinking about individual controls, CSF allows you to see the security forest.

For example, the Identify function has under its several categories: one of them being risk assessment. CSF says that while you're inventorying all your IT assets, you are supposed to also work out the risks to these assets based on the current threat environment. This is covered more specifically in the Risk Assessment category under Identify. CSF then maps the controls in this grouping into the more specific sub- controls of the standard you're using —say NIST 800-53's own risk assessment controls. It's a new way of looking at risk assessments as a key part of the asset inventory process.

And that leads to the final benefit. Through its higher-level organization, CSF forces IT to think of security as a process — a continuing program of identifying risks, putting in relevant protections, and constant monitoring. As security events are detected and responded to, the lessons learned are then fed back into the next iteration of the CSF. In short: you're always "doing security".

In this paper, we'll take a closer look at CSF, viewing it as more of a meta standard that provides mappings into the most popular data security standards, as well as helping you better manage risks through its process-oriented approach.

Let's first dive into frameworks.

FRAMEWORKS AND CSF

Repeat after me: frameworks are not data security standards! They may look similar to a data standard but they're not the same. You can think of a framework as more of a guide to help you navigate through a specific standard.

At the core of the CSF are its five functional areas. Let's list them and their NIST descriptions:

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

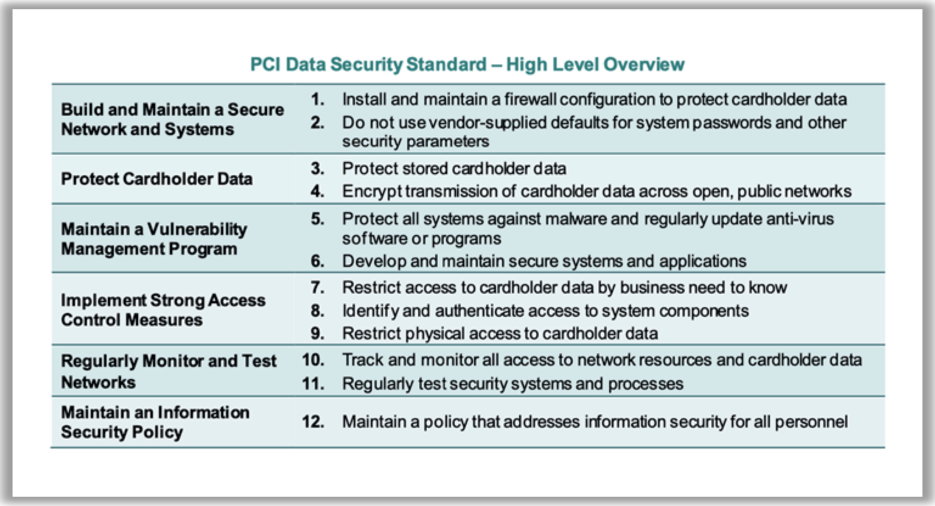
Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables timely discovery of cybersecurity events.

Respond — Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Recover — Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

These functions are at the top of the CSF hierarchy, representing the first “sorting bin”. With CSF, every security control in a specific standard can be assigned to one of these functions. There should be nothing too surprising about these particular functions since they can, often by the same or similar names, be found in many security standards. As just one example, see PCI DSS’s organization of its controls below.



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1.	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3.	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5.	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10.	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	12.	Maintain a policy that addresses information security for all personnel

When looking at the higher-level functions of PCI DSS, note that some are very specific — "Implement strong Access Controls". In the CSF classification, access controls are actually found under the far more general function of "Protect". But that's the point of CSF. It does a better job of generalizing and abstracting data security than a more specific standard!

The next levels in the hierarchy are CSF's categories and subcategories. You can think of these as additional sorting bins — specific enough so that it can meaningfully classify all kinds of standards, but not too granular so that it's as complex as the underlying standard.

For example, under Identify there are six separate security categories:

Asset Management (AM) — Identify and manage the data, personnel, devices, systems, and facilities based on their business objective and organizational risk strategy.

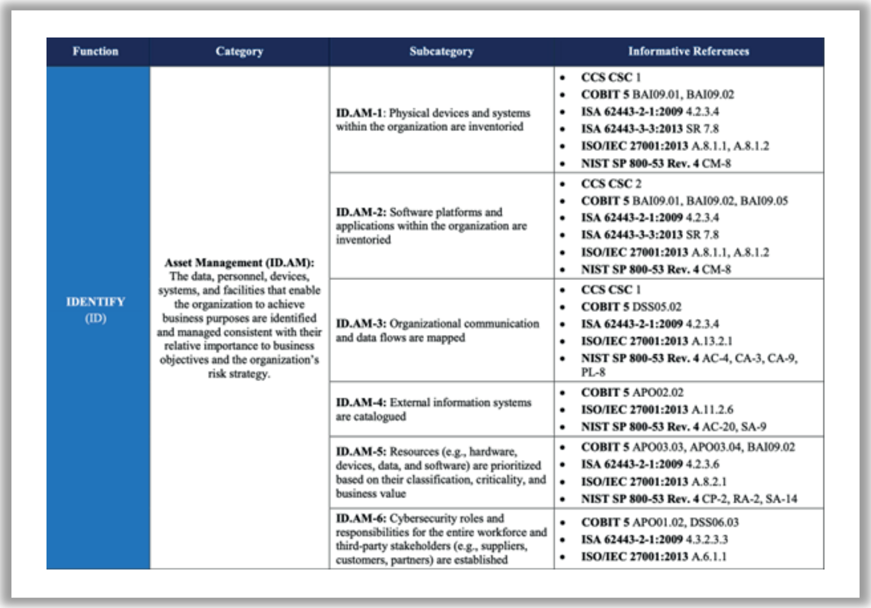
Business Environment (BE) — Prioritize organization objectives and use this to inform cyber roles and risk management decisions.

Governance (GV) — Analyze the organization's regulatory, legal, risk, environmental, and operational requirements as it relates to cybersecurity risk.

Risk Assessment (RA) — Evaluate cybersecurity risk and its impact on organization operations.

Risk Management (RM) — Establish risk tolerances and business assumptions.

At the lowest level of the hierarchy, CSF lists subcategories that finally map into the actual controls. A table is worth a thousand words, and below you'll find the mappings of the Identify function's Asset Management category broken out by its subcategories:



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

As you can see from the above table, NIST maps into many of the most popular standards. If a standard you're working with isn't listed, it's likely it has already been mapped. For example, you might notice that PCI DSS isn't mapped, but thankfully the PCI standards committee has provided the mapping in their own documentation.

The NIST CSF is not meant to be a replacement of a standard. Instead, it complements these standards by putting them into an overall security process, which we'll delve into in more detail below.

To emphasize this point, if your organization has found, say, the Mitre Att&ck Framework useful in detecting and responding to malware attacks, and has come to rely on its shared knowledge-base for real-world security, CSF doesn't force you to stop using it. The same can be said for PCI DSS and its controls, which not surprisingly, are tuned for managing credit card numbers.

All told, the NIST CSF has 23 different categories with over 108 subcategories. The following table provides a listing of the CSF classification hierarchy along with their identifying abbreviations:

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identify Management	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies & Events	DE.AE
	Security Continuous Motnioring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Migration	RS.MI
	Improvements	RS.IM

Function	Category	ID
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

THE CSF SECURITY PROCESS AND CYBER RISK

Now that we've covered the basics of CSF, let's move onto the CSF security process. It's Identify-Protect-Monitor-Respond-Recover model is better viewed as sequential steps with each step feeding into the next.

The best way to understand this is to go through a simple example.

Starting with the Identify phase, an IT department inventories file system data, say, looking for PII and then collecting associated access permissions. Other information regarding network and server configurations can be collected as well. These controls are found under Asset Management within the CSF's Identify function (ID.AM).

As we discussed earlier, CSF then requires you to conduct a risk assessment and work out how you're going to manage the risks that are discovered — ID.RA and ID.RM.

Unlike other standards, the CSF tells you that risk assessment is part of the initial Identify function.

And that means, in addition to inventorying your systems, you're also supposed to review the current threat environment, and decide those threats that are most relevant and likely to occur, and then based on an analysis of your corporate assets, select those assets whose compromise or disruption would result in the highest expected cost. In short: you're trying to get the most bang for your security investment.

The risk part of CSF is a little more complicated than we're letting on to, and to get more of a sense of it, refer to NIST'S Risk Management Framework documentation.

Protect

Let's say in this hypothetical situation, the risk analysis suggests that this company is especially vulnerable with respect to its intellectual IP — say its algorithms — that are kept in a few Windows folders.

The next stop in the NIST CSF is the Protect (PR) function, where the appropriate controls are chosen to limit access. In this scenario, the security analysts decide to focus on access rights and network integrity (PR.AC). They'll also need to put in place procedures (PR.IP) for maintaining access rights — say, explicit approval workflows for new group members — to this sensitive content. And finally, they'll need to implement these procedures with appropriate technologies — say event logging — so that unauthorized activities can be recorded (PR.PT).

So far, so good. You can see how it's easier to talk about the security process using the higher-level CSF classifications. In the background, though, the security teams will be implementing the actual controls based on the particular security standard their organization is using.

In our scenario, the IT security team decides to introduce a new Activity Directory group and puts in place procedures to manage group membership. And then the team selectively turns on various auditing features so that access can be monitored.

Detect, Respond and Beyond

Having these security controls in place is still not enough. CSF then steers us into the Detect part of the process. At this point, you decide on the software technologies that will collect events and then detect those that are anomalous (DE.AE and

DE.CEM).

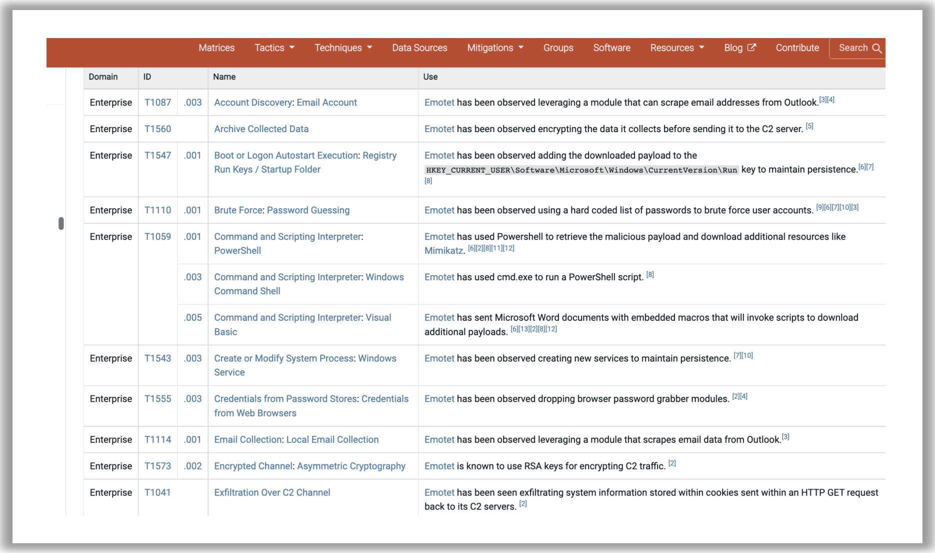
In this particular situation, we're looking for unusual and authorized access to this sensitive software related to the company's proprietary algorithms. This can be detected through abnormal file activity or network traffic on a particular server.

As we've been pointing out, CSF works in conjunction with whatever current security standard that's already in place. Let's say you're a fan of the Mitre Att&ck Framework. For groups in security operation centers (SOCs), Att&ck helps them decide the type of malware they're facing, and then how to respond. There's no issue fitting Att@ck or another approaches within CSF's Respond and Recover functions (RS.AN, RS.MI, and RC.RP).

With the controls implemented, our hypothetical organization is now ready to deal with a threat. So lets' say the SOC in our scenario, with help from Att@ck, has discovered Emotet is the malware that's infected the system and is the culprit behind some unusual file activity. Now Att@ck's knowledge base of real-world malware comes into further play. The SOC group can now look up Emotet's techniques: leveraging PowerShell scripting, searching for unencrypted user passwords, exfiltrating data to a Command-and-Control (C2) server, creating persistence through task scheduling and more.

A proper response to Emotet is a multi-step process. At a minimum, the SOC will have to disable compromised accounts, and find and stop infected software applications. Full compliance to CSF's Respond and Recover functions would also include, for Emotet, removing DLLs and malicious tasks and services, as well as deleting emails carrying infected documents.

And you're still not done! CSF is an ongoing process, and so after the malware is contained and systems have been recovered, any security shortfalls would then be addressed in the next risk assessment. In other words, in the next pass-through CSF's Identify phase, you formally address the shortfalls from the last security incidents. Security never ends!



Domain	ID		Name	Use
Enterprise	T1087	.003	Account Discovery: Email Account	Emotet has been observed leveraging a module that can scrape email addresses from Outlook.[3][4]
Enterprise	T1560		Archive Collected Data	Emotet has been observed encrypting the data it collects before sending it to the C2 server. [5]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Emotet has been observed adding the downloaded payload to the `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` key to maintain persistence.[6][7][8]
Enterprise	T1110	.001	Brute Force: Password Guessing	Emotet has been observed using a hard coded list of passwords to brute force user accounts. [9][6][7][10][3]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Emotet has used Powershell to retrieve the malicious payload and download additional resources like Mimikatz. [6][2][8][11][12]
		.003	Command and Scripting Interpreter: Windows Command Shell	Emotet has used cmd.exe to run a PowerShell script. [8]
		.005	Command and Scripting Interpreter: Visual Basic	Emotet has sent Microsoft Word documents with embedded macros that will invoke scripts to download additional payloads. [6][13][2][8][12]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Emotet has been observed creating new services to maintain persistence. [7][10]
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	Emotet has been observed dropping browser password grabber modules. [2][4]
Enterprise	T1114	.001	Email Collection: Local Email Collection	Emotet has been observed leveraging a module that scrapes email data from Outlook.[3]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	Emotet is known to use RSA keys for encrypting C2 traffic. [2]
Enterprise	T1041		Exfiltration Over C2 Channel	Emotet has been seen exfiltrating system information stored within cookies sent within an HTTP GET request back to its C2 servers. [2]

In our scenario, the Emotet incident could then lead to one of more mitigations.

It’s known that Emotet is spread through phish mails and also takes advantage of weak passwords. Besides improved security training, one obvious and powerful risk reduction technique is to audit employee passwords, say using John the Ripper, to find and improve those passwords that are crack-able.

Or since Emotet is heavily dependent on PowerShell, it may make sense to restrict access to scripting languages so as to make it more difficult for Emotet and other malware to live off the land (LoL).

In this next pass through the CSF functions, the Identify phase could now be extended to look for weak passwords as well as plaintext credentials found in the file system. And the next iteration of Protect phase could also incorporate controls to restrict access to PowerShell, using for example AppLocker, as well as limit access to other resources such as Windows services and scheduled tasks (PR.AC).

When the next security event is detected, the response will either validate the previous mitigations or else suggest new controls or refinements of existing ones.

The more important point in exploring this example is how the CSF puts data security into a larger structure, one which can be broken down into logical steps, each of which can be addressed and implemented.

REAL-WORL CSF:
RANSOMWARE PROFILE

In the above hypothetical situation, we conducted a quick risk assessment and gamed out what could happen if Emotet malware had infected IT infrastructure. Thankfully, you don't have to start from scratch in evolving a security plan for your organization!

Through their CSF profiles, NIST makes it a little easier to deal with common malware attacks, as well as security challenges faced by certain industries. The NIST profiles are tuned to address these situations — relevant controls are emphasized, and more context is provided so that defenders have a better understanding of threats.

To get a sense of how these profiles can help, it now pays to take a peek into the CSF ransomware profile. For those security groups, perhaps in smaller companies, these NIST profiles can help bring staff quickly up to date on what's important.

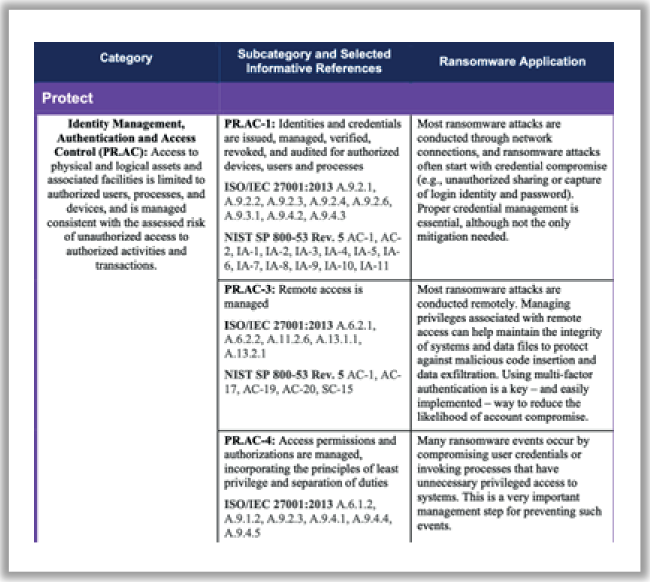
For example, the ransomware profile emphasizes in the risk assessment controls (ID.RA) that defenders consider the business impact of a successful ransomware attack, which can disrupt or even stop business operations.

So, a proper cost-benefit analysis may bring to the table more expensive and perhaps inconvenient (for the employees) defensive options: more frequent backups or mandatory use of multi-factor authentication (MFA) technologies.

The Protect function of this CSF profile also focuses on those controls that would be most relevant for ransomware. Besides recommendations for MFA, there are warnings about careless practices regarding passwords, access rights, and network access to internal resources. Again, for defenders not familiar with the new threat environment, these are important considerations.

For example, ransomware cyber thieves are known to use brute-force password attacks on public access portals — such as remote desktop — and so that makes authentication protections such as MFA likely worth the investment.

Once inside they also take advantage of broad-access rights to folders and other IT assets to allow easy lateral movement, and then ultimately to the file system. The CSF ransomware profile focuses on these ideas in the PR.AC and PR.PT subcategories.



Category	Subcategory and Selected Informative References	Ransomware Application
Protect		
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 5** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	Most ransomware attacks are conducted through network connections, and ransomware attacks often start with credential compromise (e.g., unauthorized sharing or capture of login identity and password). Proper credential management is essential, although not the only mitigation needed.
	PR.AC-3: Remote access is managed **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 5** AC-1, AC-17, AC-19, AC-20, SC-15	Most ransomware attacks are conducted remotely. Managing privileges associated with remote access can help maintain the integrity of systems and data files to protect against malicious code insertion and data exfiltration. Using multi-factor authentication is a key – and easily implemented – way to reduce the likelihood of account compromise.
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	Many ransomware events occur by compromising user credentials or invoking processes that have unnecessary privileged access to systems. This is a very important management step for preventing such events.

Finally, the Respond and Recover sections of the profile provides additional pointers on the legal and regulatory aspects of an attack.

In the case of ransomware, there are other resources to tap into, some listed at the end of the profile documentation. In addition, our own Complete Guide to Ransomware has practical real-world advice on detecting and responding to ransomware.

To re-emphasize, the NIST CSF is a high-level guide to the standards, placing security controls into a larger process. You still stay with the existing data security standards, but use CSF, along with its specific profiles, as part of a process that continually adjusts security based on new information gathered from the previous phase.

DATA SECURITY PLATFORM (DSP) TECHNOLOGIES AND CONCLUSION

While you can initially leverage in-house resources and staff to carry out a data security program, in the longer term it's make far more sense to purchase business-class software product. Even for some of the simpler controls recommended by various standards, such as least privilege access for files or implementing event audit logs, the software required to collect and analyze this information is typically beyond the skills of most organizations.

These and other arguments lead to the necessity of a data security platform or DSP. It's an integrated software solution that can automate some of the key security processes in the NIST CSF model, especially in the Identify and Detection phases.

DSPs are also very useful in CSF's Detect phase. The information that the DSP collects from user activities and internal system events are fed into advanced statistical or AI algorithms that then decide whether an attack is underway. This technique is known as user behavior analytics (UBA) and involves developing a profile of common file and process activities for each user.

With a UBA profile in hand, the AI algorithms then decide whether a sudden flurry of, say, file accesses preceded by unusual use of PowerShell functions or updates to the Windows registry is normal — which might be the case for, say, an admin conducting system maintenances — or unusual and possibly the indication of an attack if the activities are associated with ordinary user.

DSPs give security specialists and SOCs a deep window into an organization's IT assets and their permissions, along with access activities on a per user basis as well as other system event information. In a single solution, DSPs can help make accurate risk assessments, automate appropriate access and other security controls, and then monitor the results.

This all fits hand in glove with the NIST CSF and its process model for risk reduction. The CSF provides the overall direction of your security, and a DSP automates its controls. It's a powerful combination!

If you have any questions about the NIST CSF or want to learn more about our own data security platform, contact a Lepide representative today.

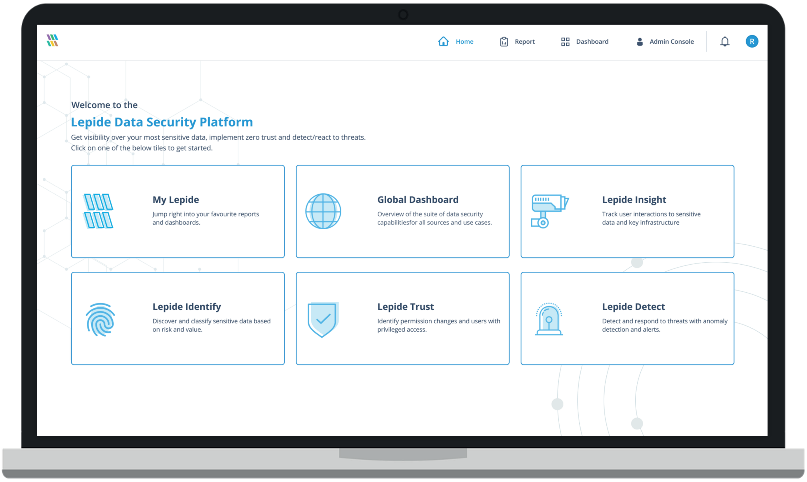
ABOUT LEPIDE

We founded Lepide back in 2015 because we felt cybersecurity was failing to keep up with the rapidly changing market. It lacked context and intelligence and was failing to protect what really mattered – the data.

Fast forward to today, and we have over 1,600 happy customers all over the world using our award-winning Data Security Platform.

Data breaches, including those associated with ransomware, often start with Active Directory, with attackers moving laterally within the network to target sensitive data in file servers and other data stores.

Our unique approach, and our powerful solution, provides the much needed visibility over changes to these critical systems and interactions with sensitive data. We deliver this information in real time to enable you to quickly detect and react to security threats.



Welcome to the

Lepide Data Security Platform

Get visibility over your most sensitive data, implement zero trust and detect/react to threats.
Click on one of the below tiles to get started.

My Lepide
Jump right into your favourite reports and dashboards.

Global Dashboard
Overview of the suite of data security capabilitiesfor all sources and use cases.

Lepide Insight
Track user interactions to sensitive data and key infrastructure

Lepide Identify
Discover and classify sensitive data based on risk and value.

Lepide Trust
Identify permission changes and users with privileged access.

Lepide Detect
Detect and respond to threats with anomaly detection and alerts.

If you'd like to take a closer look at Lepide Data Security Platform, we recommend the first place to start is a personalized demonstration.

If you're more interested in detecting and preventing threats in your environment immediately, then we suggest to schedule a free risk assessment session with one of our security team.

Follow the links below:

https://www.lepide.com/demorequest.html

https://www.lepide.com/data-risk-assessment.html

THANKS FOR READING

Lepide