Red River

HOW MANAGED DETECTION & RESPONSE HELPS YOU ACHIEVE COMPLIANCE

PCI, GDPR, HIPAA — companies today are facing an ever-growing list of regulations. As compliance becomes ever more difficult to maintain, what can organizations do to protect themselves and their bottom line? Regardless of industry, compliance can be life or death for a business. In industries such as federal contracting and government work, it's absolutely critical. Organizations need to pass their compliance audits, or they're out of business.

Managed Detection and Response can help.

FROM HIPAA TO PCI: THE CHALLENGES OF SECURITY COMPLIANCE

Imagine an immense network: thousands of computers, routers, firewalls, mobile devices, smart devices and IoT devices. Each of these components is under the constant threat of attack. If any of them are compromised individually, it could mean that the entirety of the network is compromised. And these components are not static: Day by day, devices are taken offline, and new devices requisitioned. The network is a living, breathing thing, constantly changing and constantly threatened.

Today's organizations are under extraordinary pressures. They need to maintain their security and privacy. They need to meet compliance, from HIPAA to GDPR. And they also need to do business: They need to remain productive, functional and cost-effective. And all this means that they need to be able to more effectively manage and monitor their devices — a task that simply isn't always possible to do in-house.

It's not enough to improve security once. Organizations have to be continuously conscientious. Organizations have to foster a culture of security; they have to be able to constantly update their compliance knowledge and proactively improve upon their compliance. They need to be able to identify challenges and pain points, and they have to be able to address those challenges in a structured, iterative fashion. When a security incident does occur, the organization must be able to respond to that incident with swiftness.

But so many organizations are already stretched thin. Security isn't a revenue-generating activity, and consequently, may not be prioritized.

IT employees may not feel as though they have the time or resources to research and improve upon security compliance. They may update infrequently, or may wait until there's an incident to audit their security processes. But the truth is that periodic security updates are faster and more affordable; the more the organization remains on top of compliance, the less likely it is that a time-consuming issue might occur.

Managed Detection and Response can help an organization achieve multiple types of compliance:

- **PCI DSS.** Integrate software, analytics and expert security systems to ensure controls required for Payment Card Industry (PCI) DSS compliance. PCI DSS is the standard for organizations handling branded credit cards. The Payment Card Industry Security Standards Council controls these regulations, and is serious about them — they manage the payment information for millions of card holders.

- **GDPR.** Implement full GDPR compliance. General Data Protection Regulation (GDPR) has a number of technical control requirements for how the personal information of EU citizens is stored and accessed. Organizations need to be able to ensure that EU citizens are properly notified regarding how data is being stored and used, and make sure that this data is constantly protected.

- **HIPAA.** Deploy advanced solutions to secure medical and personally identifiable information, achieving HIPAA compliance, HITECH and mandates for Meaningful Use. Organizations need to keep up with HIPAA compliance if they are storing personal medical information.

- **SOC 2.** Integrate systems with asset discovery, vulnerability assessment, threat detection and application security. The SOC 2 compliance is a special auditing procedure that provides baseline governance regarding data security. SaaS service providers should meet SOC 2 compliance, as should any other third-party vendors.

- **SOX.** Increase accountability and reporting, while improving security audits through SOX compliance. SOX compliance requires that internal controls meet reporting standards, that safeguards have been established for data handling and that someone is responsible and accountable for security issues.

Not every organization needs to meet every compliance standard, nor does every organization need to meet the most rigorous requirements of these standards. But an independent assessment through a security auditor will tell an organization which standards it has to meet and what may be holding it back from compliance. It is every organization’s responsibility to find out what security standards it needs to meet, and to ensure that it is able to meet them both now and moving into the future.

ACHIEVING BETTER COMPLIANCE THROUGH MANAGED DETECTION AND RESPONSE

When there are thousands of end points on a network, they have to be individually monitored. Through Managed Detection and Response, software can be placed on all devices to look for potential problems and report these problems to a central location. Managed Detection and Response (MDR) alleviates many of the pressures on an organization by outsourcing the most vital elements of compliance to a third party with superior knowledge and resources.

MDR solutions detect problems, log those problems and send notifications to a dashboard — usually a universal dashboard that either a managed services provider or the organization's own internal IT will monitor. A comprehensive MDR solution provides everything an organization needs to show that it is remaining compliant, insofar as it is responding swiftly to threats, and that it has the technology and protocols in place to identify those threats. And with a third-party administrator, these MDR solutions can also be administered outside of the company — ensuring that experts are always empowered to react to security threats.

The MDR dashboard provides a first layer of support, by categorizing issues based on risk level. Administrators are able to review every security or compliance issue at a glance, and are able to address the highest risk issues first. Organizations are able to deploy an MDR dashboard and either use their own in-house IT department or external administrators to manage it. As MDR systems grow in complexity and intelligence, they are able to better gauge the risk level and optimal response for each incident.

Because infrastructures do grow more complex over time, security and compliance solutions need to be scalable. Managed Detection & Response is a scalable solution, as it is an outsourced one; the MSP is able to identify issues as they occur and only escalate issues as needed. MDR ensures that the company is able to focus on other areas of internal compliance rather than having to respond to security incidents one by one. Because of this, MDR frees an organization up to scale as desired, without having to worry about bolstering its in-house resources.

AUDITING YOUR ORGANIZATION'S VULNERABILITIES AND COMPLIANCE

It's not always easy for an organization to identify its own vulnerabilities or issues with compliance. The easiest way for an organization to find out more about where it's at in terms of security is to go through a security audit. Independent auditors can assess whether vulnerabilities are being properly addressed and whether best practices are followed. Where the organization is discovered to be lacking, the auditor can make suggestions based on standards and best practices.

A pre-audit assessment company can be engaged to identify the organization's pain points and challenges. Commonly, organizations are hanging on to outdated technology, employees aren't being trained effectively or the IT department is spending too much time putting out fires to even begin to address issues of compliance. The pre-audit assessment will cover any areas in which the company isn't achieving compliance, and will move forward to identify what the organization can do to improve upon those areas.

After the pre-audit assessment, a remediation project begins. The goal of the remediation project is to address any issues that were found by the audit, whether they use the audit's recommendations, their own internal recommendations or the recommendations of other experts.

Finally, an oversight committee makes sure that the holes that were discovered have been properly plugged. Using the pre-audit assessment, they will work with the remediation team to ensure that everything that was discovered was addressed. Moreover, the oversight committee will also work to ensure that these types of issues don't occur again. Everything will be double-checked, or even triple-checked, to make sure that the organization's compliance issues have all been resolved.

MORE EYES AND HANDS LEAD TO BETTER COMPLIANCE

Over time, many organizations find themselves becoming steadily more vulnerable to issues of security and compliance. When IT is only being managed internally, IT teams may not have the time necessary to improve their security. They may be overwhelmed by daily tasks and putting out fires, or may just acquire gaps in their security because of their own blind spots. If the IT staff isn't constantly having their knowledge refreshed, they may not even be aware of new threats as they emerge.

During the process of IT auditing, more hands and eyes are on the IT infrastructure as a whole. Managed Detection and Response teams are able to go over the organization's current processes to improve them, and can work to help with monitoring and management moving forward. Internal IT departments are given the technology they need to facilitate better, easier and faster security and privacy, while external IT departments are able to leverage their own, often superior technology.

External security and compliance analysis is critical for any organization dealing with privileged data. A Managed Detection and Response team often provides the additional eyes and hands an organization needs to identify and deal with issues of regulatory compliance.

IMPROVING COMPLIANCE THROUGH SUPERIOR TECHNOLOGY

Many organizations operate with legacy solutions — even if they feel as though they should be upgrading their technology. As much as 75% of IT spending is spent supporting legacy solutions that organizations feel they don't have the time or expertise to move away from. Legacy solutions aren't just an issue because of productivity. They're a problem because of compliance and security.

Older software solutions aren't likely to be well-secured or meet current compliance. An old software solution, for instance, might not have multi-factor authentication available. Thus, their login may be inherently not secure, even if users are doing everything they can to make it secure.

Physical hardware devices that are no longer supported aren't going to be patched, and any vulnerabilities that have been discovered are going to be highly visible to malicious attackers. And it isn't just devices that are very old that can become vulnerable. IoT devices manufactured just a few years ago are often easily compromised, and their compromise could easily lead to the compromise of an entire network.

Even when legacy solutions aren't being used, modern systems have to be regularly patched and configured to remain secure. Many IT departments fail to update their devices as frequently as they need to, because they don't feel they have time for this routine maintenance. In fact, many organizations aren't even keeping up-to-date backups for the same reason. Organizations need to be able to consistently update and patch their software and hardware to remain compliant, which is again a routine, mundane task that can be outsourced to a third-party compliance expert.

With better technology such as mobile device management platforms, organizations are able to better manage their smart devices and IoT solutions. Technology can be used to improve compliance by providing compliance-focused dashboards and analysis. Compliance-focused solutions are able to track compliance on a granular level and ensure that a company is reporting compliance as it should. The better the technology is, the easier it will be for internal IT departments to manage their compliance.

Managed Detection and Response provides a complete, all-in-one platform linked directly to devices, to ensure that they are managed and monitored effectively. Through MDR, companies are able to quickly identify the devices that aren't working properly, could be compromised or need to be updated for greater levels of compliance. Managed Detection and Response teams are then able to resolve issues as quickly as possible, in order of priority.

GETTING STARTED WITH MANAGED DETECTION AND RESPONSE

Remediation services dig deep into an existing infrastructure to determine whether there are security concerns that have to be addressed. Remediation teams first look at the organization to identify any major pain points, challenges and risks. From there, they will make recommendations regarding changes that would be necessary for the organization to be in compliance. And once those recommendations have been made, the remediation services will go and investigate further, to ensure that everything has been appropriately changed.

If an organization is concerned about achieving the compliance they need at cost-effective prices, Managed Detection and Response is often the best solution. Managed Detection and Response offers the technology and experience that organizations need to achieve compliance, without the organization itself having to invest in bolstering its own internal IT team.

Compliance needs are going to be constantly changing, and companies need to be ready, willing, and able to change with them. By investing in compliance, organizations protect themselves in the future — as well as employees, vendors and clients. Managed Detection and Response is one of many ways an organization is able to improve upon its security and privacy, while still avoiding a significant increase in the cost of its operations.

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing 25 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions. To learn more, visit redriver.com.