EXECUTIVE BRIEF

Protect or Perish:

Why your organization needs a Defense-in-Depth solution to secure your critical information assets

In this paper:

- True digital resilience demands a hardened security posture that identifies risk both inside and outside your organization.
- A robust security strategy means deploying a layered solution that tracks, monitors, and hardens your network environment to assess threats you know exist-and the ones you haven't imagined yet.
- In addition to network security, a Defense-in-Depth approach demands that you know exactly where and how your sensitive data is stored, how it is accessed, and who can access it.
- A solution that monitors and tracks both your data and your network security gives you 360-degree visibility and the power to protect your entire network.

Modern IT professionals are true multitaskers. From meeting security, compliance, and regulatory demands, to provisioning hardware and controlling costs, organizations rely on their IT leaders to keep the business up and running.

Any organization that deals with data (in other words, just about everyone) must take steps to protect and monitor the security of their networks. For some IT pros, that process starts by deploying point solutions (like firewalls and single-use software packages). Others take security a step further with a security information and event management service (SIEM).

But point solutions or a SIEM alone cannot provide a fully secure environment, and could even provide a false sense of security. The bottom line is that generating alerts isn't enough. It's critical to make sure the right resources are deployed to protect, monitor, and test the network. A robust solution identifies and prioritizes alerts effectively by utilizing built-in expertise that guides the organization to take action whenever needed to protect the entire environment.

At the same time, a SIEM alone cannot dive into the specifics of an organization's data and documents. Organizations need to store sensitive data such as personally identifiable information (PII) securely so as not to risk steep regulatory fines. They must manage access to documents and data to track unauthorized or unusual activity, and to keep current with business changes. Finally, they could be wasting valuable (and expensive) storage space by storing data unnecessarily in multiple locations, or by storing data that is out of date or otherwise unusable. These oversights drain resources without adding value.

More data to manage can lead to more risk for your organization.

Protecting your organization's data can feel like chasing a moving target. Threats from malicious actors continue to multiply, while the sheer amount of data being generated continues to increase exponentially. According to Forbes, since May 2018, 2.5 quintillion bytes of data have been created every day. An astounding 90% of the world's existing data was created in just the last two years.[i] By the year 2025 we will be drowning in over 175 zettabytes (ZB) of data (for context, one ZB equals one trillion gigabytes), according to a study by IDC.[ii] And all of that data needs to be protected and monitored to meet the demands of both organizational security and regulatory compliance.

The risk, safety, and security of your data is the number one prioirty when you are planning your business, because if there is an interruption to it, you have no business.

Every organization knows that monitoring and protecting its networks is crucial to data security. However, organizations with a network security strategy in place may only be solving for half the puzzle without monitoring sensitive business data for compliance requirements, access controls, and usability as well. It's easy to overlook the necessity of having a strong security posture for data and documents—but that oversight could blindside you and negatively impact business processes, operations, and even your competitive position in the marketplace.

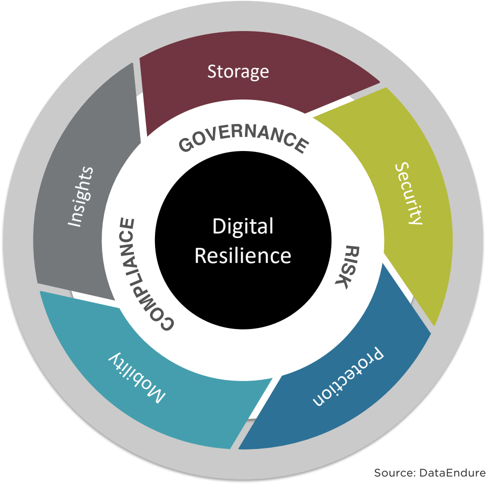
Is your data safe? You need to be able to say "yes" confidently, 24/7.

"Not doing anything" to protect your data can cost your organization. Consider GDPR fines alone: total penalties levied to organizations up to August 2019 totaled a whopping $294 million. Over $2 million annually is lost per year, per organization, to data management issues. A full 83% of IT professionals report that siloed data management is impacting their compliance efforts, and 85% cite the potential loss of personally identifiable information (PII) as a top concern. Almost half of IT decision makers in a recent study said they were most worried about a potential security breach.[iii] It's clear that every organization, regardless of size, must take data security today just as seriously as network security, or risk the results of a breach.

Mike Fisher, COO of Therma, puts it succinctly. "I struggle all the time with that balance [between innovation and security]," he notes. "[But] It's not a balance. The risk, safety, and security of your data is the number one priority when you are planning your business, because if there is an interruption to it, you have no business."

Network and data security: A defense-in-depth approach to digital resilience

It's no longer enough to build a "security strategy" for your organization. Today's IT leaders need to embrace a strategy of digital resilience. True digital resilience is more than just a hardened security posture. It's a comprehensive way of thinking about how modern organizations can manage effectively in an always-on, 24/7 digital world, while protecting their crucial digital assets.



Source: DataEndure

A digital resilience strategy:

- Protects your data from compromise, and enables you to recover quickly and keep your doors open even if you are under attack.
- Gives you full visibility into your environment in real time.
- Allows you to control access to your networks, documents, and data.

- Alerts you to unusual user activity quickly to head off potential attacks.
- Allows you to access, analyze, protect, and make informed decisions based on your data, no matter where it is located.

> “I can’t think of any other time when IT leaders have been operating under so much pressure dealing with so much change.”
>
> John Gallant, IDG Strategies

Protect your network with a Security Operations Center (SOC) as a Service

A SOC-as-a-Service (SOCaaS) offers many benefits over and above point solutions that merely generate alerts. A robust managed security offering allows you access to security experts who monitor your networks in real time, with alert prioritization, continuous updates, and regular testing. Proactively seeking out potential weaknesses in your network allows you to strengthen defenses to prevent a potentially crippling attack.

A robust SOC-as-a-Service gives your organization:

- Full 24/7 visibility into the health of your network, systems and security controls.
- Actionable alerts distilled from thousands of events, backed up by a dedicated SIEM with security log aggregation, correlation and management.
- A full understanding of network flows and live traffic; advanced threat intelligence; and continuous vulnerability assessments.
- Constantly-updated security protocols to ensure your SOCaaS can quickly detect the most timely threats.

Protect your documents and data with an integrated information intelligence tool

A comprehensive intelligent data platform allows you full visibility into all of your data and documents worldwide. It allows you to visualize where your critical and business-sensitive information lies—and where it could be at risk. Organize your data and take informed action so that your organization can be confidently prepared to handle security concerns, compliance regulations, and continuous data growth to ultimately regain control of your data.

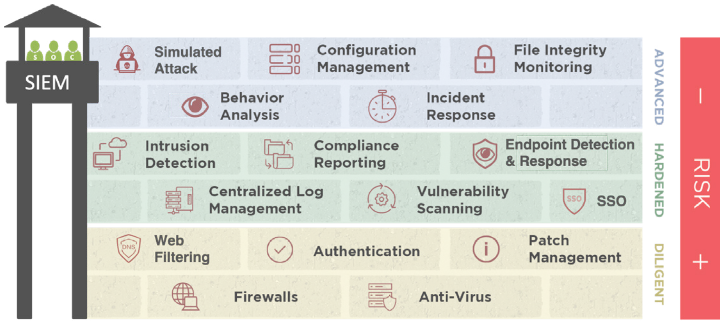
A strong data platform allows your organization to:

- Identify stale, risky and unnecessarily kept data to address data privacy and compliance regulations.
- Identify valuable data that’s currently buried.
- Access a variety of data connectors to gain a comprehensive view of your data.
- Make informed actions on data that mitigate compliance risk and free up or eliminate unnecessary storage.
- Take advantage of robust file analysis tools that aggregate your metadata to better understand your data.

The value of partnership: DataEndure SOC-as-a-Service and Veritas Information Studio

While literally thousands of managed service providers offer point solutions for network security, very few providers are offering a 360-degree solution with layered protection for data and document security. Yet, it's this powerful combination of integrated network and data security solutions that provides the greatest level of security and visibility. The combination of a robust SOC-as-a-Service monitoring your networks and an intelligent data platform analyzing and optimizing your data creates a fully-visible environment where you can quickly identify opportunities for optimization, ensure regulatory compliance, and mitigate against threats inside and outside your organization.

Together, DataEndure's SOC-as-a-Service and Veritas' Information Studio provide:



- A layered security approach with multiple facets that provide a holistic view of your entire global network and all data and documents, so you can access and understand your complete environment in one view.
- Real-time visibility into key network and data telemetry to help identify the full scope of anomalies, risks, and threats.
- An overall strengthened security posture that puts your organization on the offensive against cyber threats.

Take the next step towards digital resilience.

Learn more about how DataEndure and Veritas can help you manage your digital resilience strategy with an integrated DataEndure SOCaaS with Veritas Information Studio. Contact DataEndure today for a free Security Assessment to get started.

About DataEndure

DataEndure is in the business of successful outcomes. Most people can't believe it when we say that we've been in business for over 35 years. We have grown up with the industry, which gives us unique expertise that we use to help your business bypass traditional data challenges, zoning straight in for what really will or won't work for you. We bring together the gold standard of technological insight and capabilities with the ethics and heart of a family business, right here in Silicon Valley. For three generations now, we are proud to be the home of secure, smarter, and cost-effective IT solutions. Learn more at www.dataendure.com.

About Veritas

Veritas is a global leader in data protection and availability. Over fifty thousand enterprises rely on us to abstract IT complexity and simplify data management. Veritas' Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights needed to comply with data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas supports more than 500 data sources and over 150 storage targets, including 60 clouds. Learn more at www.veritas.com.

[i] https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#18f5ce7860ba

[ii] https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html

[iii] https://www.techrepublic.com/article/why-data-security-is-now-a-top-concern-for-it-leaders/