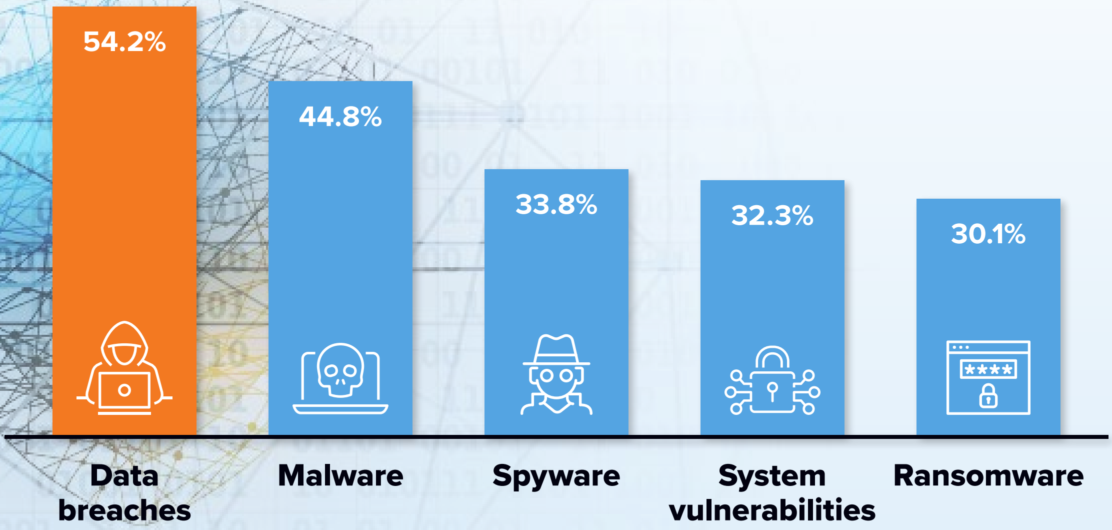
Adaptive Multi-layered Defense Is the Key to Cyber-Resiliency

The widespread impact of a data breach is a top of mind concern for organizations.

Top Enterprise Cybersecurity Concerns



Source: IDC, MSSP Survey 2019 | n = 402

As organizations across the globe struggle to tackle the operational, strategic and financial impact of COVID-19, more agile and growth-centric organizations have seen this as an opportunity to leapfrog competitors within their specific industries and bring new products and experiences to their customers. These organizations embrace enterprise resiliency and the need to “pivot” to grow their business when faced with adversities.

These organizations are in the process of executing transformation strategies during the crisis that offer enhanced digital experiences and dramatically change the way in which they interact with their customers as well as partners. In fact, many organizations today are borderless entities that give customers, employees, partners, and suppliers anytime, anywhere access to corporate resources.

In order to deliver digital experiences to these constituents, organizations have had to embrace and become digitally driven organizations themselves. In response, organizations are investing in technologies that enable more agile business operations and shifting to the cloud as core to their IT operations going forward.

Within these organizations, data has truly become the “new gold” that fuels the business. Access to that data has become equally important to provide key business insight, make faster decisions in response to market changes, and to stay in tune with customer needs and requirements. However, due to the value of data, and risks associated to the data being compromised, devising comprehensive strategies to protect against a data breach has become a key business imperative.

In the new digital paradigm, corporate data and applications are spread throughout the organization and exist in traditional datacenters, public clouds, and private cloud. While providing anywhere, anytime access to corporate resources is viewed as a means of driving efficiency, speed, and flexibility, the challenge of both securing data and access to data has become much more difficult due to the sheer volume and distribution of data.

IDC surveyed 400 enterprises to learn about their top cybersecurity concerns. Nearly 55% of the respondents indicated that data breaches were the biggest concern. The ramifications of a data breach are far-reaching. In addition to potential fines incurred by violating data protection mandates, and/or legal liability that the organization must bear, the damage to the company’s brand and reputation due to the loss of trust from customers can have a long-term impact.

Subsequently, enterprises are placing greater emphasis on implementing the proper technologies to protect data and applications, as well as updating out-of-date policies and procedures for effectively granting access privileges to corporate data wherever it resides.

Message from the Sponsor

Cyber resilience is the ability of an organization to enable business acceleration (enterprise resiliency) by preparing for, responding to, and recovering from cyber threats. A cyber-resilient organization can adapt to known and unknown crises, threats, adversities, and challenges. The ultimate goal of cyber resiliency is to help an organization thrive in the face of adverse conditions (crisis, pandemic, financial volatility, etc.).

Micro Focus develops integrated cybersecurity solutions to enhance your intelligence and cyber resilience and protect against advanced cyberthreats at scale. Learn more about becoming cyber resilient…

Take Our 360 Degree Assessment

The Challenge of Emerging Trends

Going forward, the challenge of building an effective data protection strategy will become more difficult as organizations must consider emerging trends that will have a significant impact on how best to manage data, applications, and identities. These include:

- **Privacy regulations** and the need to adhere to increased complexities they introduce
- **Software supply chains** and the shift required to ensure secure code is embedded into in the software development lifecycle
- **Accelerated digital transformation** with the movement of enterprise applications between cloud/multi-cloud and on-prem domains
- **The proliferation of connected devices** brought about by greater adoption of IoT
- **Digital identities** and ensuring appropriate governance no matter whether human or a technical element

A key component of establishing cyber-resiliency is having a comprehensive strategy for data and application protection. This means having an understanding of the value of data to the business, the liability/risks associated with data, where data resides in the organization, appropriately classifying data, and understanding the dynamic and distributed nature of data. Having this 360-degree view of data allows for effective decision making on implementing the appropriate technologies, policies and procedures needed for data protection.

All IDC research is © 2020 by IDC. All rights reserved. All IDC materials are licensed with IDC’s permission and in no way does the use or publication of IDC research indicate IDC’s endorsement of Micro Focus’s products or strategies.