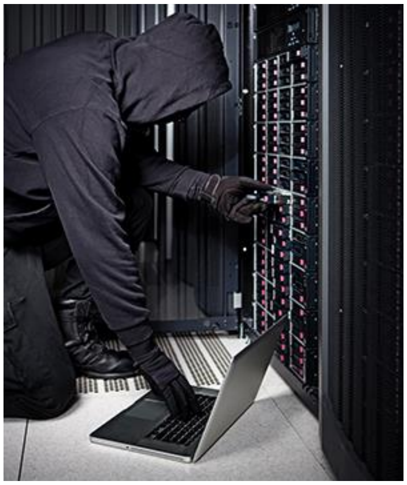
www.pipelinepub.com
Volume 18, Issue 1

A Look at 2022 Enterprise Security Strategy

By: Vlad Friedman



With the complexity and frequency of security incidents and data breaches on the rise among enterprises, these organizations and the data centers that support them need to protect critical data by maintaining continuous monitoring of security and compliance practices into 2022 and beyond.

Industry officials point to the practices of the most effective data center companies that leverage in-house expertise and infrastructure platforms to thwart malware and malicious activity. All the while, data centers need to adhere to industry regulations and requirements, which in the long run can further reduce the burden on IT staff and budget at the enterprise level.

Gone viral

Anti-virus protection plays a fundamental role in any enterprise security strategy and provides a strong first-line defense in stopping malicious activity before it enters the network. To keep up with these evolving threats, hosted infrastructure needs an anti-virus solution that offers best practices, as well as the best technologies.

A managed antivirus solution delivers both. It combines deep machine learning with endpoint detection and response to provide unmatched protection against malware, exploits, and ransomware. Data center security experts need to be able to install, calibrate, configure, monitor, and operate comprehensive anti-virus systems across an enterprise's hosted infrastructures, driving operational excellence and governance for organizations while keeping costs stable and predictable.

Exploiting prevention

The most effective anti-virus protection provides comprehensive exploitation prevention by blocking the techniques used to distribute malware, steal credentials, and escape detection, enabling organizations to ward off evasive hackers and zero-day attacks.

Distributed denial of service (DDoS) attacks are among the most debilitating threats that IT infrastructure can face and successfully fending them off requires the right technology and partners. The best responses leverage smart technologies to eliminate DDoS attacks in real-time, including both stealthy, sub-saturating attacks and volumetric attacks. They allow friendly user traffic to flow uninterrupted and keep applications and services continuously online, even while under attack.

With DDoS mitigation services, enterprises can turn their attention to the core business, knowing that their hosted IT infrastructure is safe from network-layer DDoS attacks—all the while reducing operational costs while improving performance.

Real-time detection and mediation

A secure hybrid IT infrastructure starts at the perimeter—or the network edge. Intrusion detection and prevention services (IDS/IPS) are a crucial element of perimeter protection, ensuring proactive security and a quicker response to threats. The best IDS/IPS solutions in 2022 will use a combination of technologies, including deep packet inspection, threat reputation, URL reputation, and advanced malware analysis on a flow-by-flow basis. This provides comprehensive perimeter threat protection against known and undisclosed (zero day) vulnerabilities, malware, ransomware, and phishing.

Managed IDS/IPS solutions are designed to identify and block malicious traffic, prevent lateral movement of malware, ensure network availability and resiliency, and enhance network performance. The service leverages machine learning and statistical data modeling, malware filters, and a reputation feed that identifies known bad IP addresses, DNS names, and URLs, thereby blocking malware-infected machines from contacting their command and control (CnC) hosts.

Protecting applications and enhancing performance

Web application firewalls are traditionally the first line of defense for protecting web-based applications in a hybrid or hosted infrastructure. But monitoring them and keeping them up to date can consume valuable IT resources. A managed web application firewall service provides continuous perimeter security site speed and performance through advanced caching and load-balancing mechanisms, leading to websites that are safer, faster, and more resilient.

Managed web application firewalls filter, monitor, and block HTTP traffic to and from an enterprise's web application. Look for more of these firewalls in 2022, to the extent that each request to the WAF is inspected against a rule engine that is continuously updated with signature-based heuristics, IP reputation, and threat intelligence curated from global networks. Suspicious requests can be blocked, challenged or logged, while legitimate requests are routed to the destination. Integrated load balancing and caching can speed the delivery of content and enhance the overall end-user experience.

Create a zero-trust security platform

Confirming the identity of users before they access critical applications and data is an absolute necessity for securing hybrid IT infrastructure. Multifactor solutions add an additional layer of access control to enterprise-hosted IT systems by making sure users are who they say they are and protecting you against phishing and other access threats.

As data centers and enterprises move into 2022, two-factor authentication platforms will become more prevalent, confirming any user on any type of device, anytime, and anywhere. This allows enterprises to create a true zero-trust security profile where all users—whether inside or outside of the infrastructure—must be verified. It also provides the endpoint visibility that companies need to get control of devices and the policy management needed to maintain compliance.

Those tools should include:

- **Multifactor authentication:** Utilizes a variety of methods to verify user identities including Universal 2nd Factor (U2F) tokens, mobile passcodes, or phone confirmation.

- **Policy enforcement:** Allows enterprises to set fine-grained policies to grant or block access attempts based on a user's role, device hygiene, location, network, and a host of other contextual factors.

- **Compliance enablement:** Confirms users' devices meet your security standards before granting them access, helping you meet compliance requirements.

Compliance is pivotal and remains complex and ever-changing. Accreditations are critical in measuring standardized approaches to security and risk assessment, authorization, and continuous monitoring, essential for organizations in the digital age. Leaders from companies like DataBank point to the primary importance of ensuring compliance to make sure that customers have the tools, resources, and solutions they need to keep their data private and secure.

Among these, and possibly most important, FedRAMP is General Services Administration's (GSA) Federal Risk and Authorization Management Program, providing a standardized approach to security and risk assessment, authorization, and continuous monitoring, which are essential for organizations in this digital age. For this, data centers need an authorization to operate (ATO) from multiple U.S. federal agencies, as they support healthcare organizations, financial services companies, merchants, and SaaS providers, helping them to keep their infrastructure, websites, and applications compliant. Key certifications come from organizations like FISMA, SSAE18, SOC1, SOC2, HIPAA, PCI-DSS, and Privacy Shield—GDPR and the PCI Report on Compliance (ROC).

Looking ahead, a new certification will soon be available, building on the FedRAMP requirement. The Cybersecurity Maturity Model Certification (CMMC) will review and combine various cybersecurity standards and best practices under one security framework for the entire DoD. Although the DoD is going with the CMMC as their standard, it is not discontinuing the FedRAMP model and will view certain levels of FedRAMP as compliant with the CMMC. These standards will be mapped across levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.

Even with the specter of malware and security breaches as a bit of an industry overhang, the prognosis is good. Data will be stored and shared more safely and the relationship between the data center and the enterprise will only strengthen in 2022, as both use an increasingly diverse and sophisticated set of managed services and security tools.