INFINITELY VIRTUAL

E.V.E. Advantage – Security

A cloud hosting environment with powerful built-in security features

Cloud hosting environments differ in many ways, not least of which is the level of security they include to keep your applications and data safe. Many cloud providers simply offer computing power and connectivity. If you want strong security features on top of that, it's on you to purchase the necessary solutions, set them up, and maintain them.

Infinitely Virtual (IV) took an intentional, customer-centric, and security-focused approach to designing the Enterprise Virtualization Environment™ (E.V.E.), our proprietary cloud platform that delivers 100% uptime, absolute data protection, and unlimited scalability. Recognizing that safeguarding customer data is a top priority, we make design choices to ensure the information in our environment is always protected against modification, damage, loss, or theft.

A key advantage of E.V.E. is its wide range of robust security features — most of which are included in our monthly hosting fee. IV closely monitors the ever-changing cyber-threat landscape and implements the latest best-in-class security technology to ensure optimal protection for our customers.

Physically Secure Data Centers

E.V.E. is located in carefully selected data centers that employ state-of-the-art physical security technology. The data centers are protected by an eight-foot perimeter fence and are monitored by exterior and interior cameras with IP (Internet Protocol) DVRs. To enter the primary or secondary data center facility, one must first pass through a mantrap, operated 24x7 by security guards, and managed by both keycard and biometric access control. Entry to each floor and suite is controlled by keycard.

Within the data centers, physical access to E.V.E. is restricted to employees of Infinitely Virtual. Both the physical data centers and the E.V.E environment undergo SSAE 18 SOC Type 2 and HIPPA audits annually.

Best-in-Class Technology

IV is constantly evaluating and adopting best-in-class technologies to ensure optimal security for our customers. For example, when we first designed E.V.E. in 2006, we used state-of-the-art Intel® processors. Much to the surprise of the IT industry, Intel chips were found to have critical vulnerabilities that allowed attackers to steal data from the memory of running applications. Then, when a fix was released, it resulted in a performance degradation of up to 40%, Deeming this "fix" to be unacceptable, IV immediately started transitioning from Intel to AMD processors, which feature a security mechanism that supports data encryption at the chip level and while traveling across the memory bus.

Today, E.V.E. features AMD processors because they offer what we believe to be the most secure computing option currently available on the market. As E.V.E. continues to evolve, we will make technology choices based on capabilities, including those related to security, rather than brand.

Firewalls

Every IV customer's hosting environment is protected, at a minimum, behind our carrier-grade Juniper SRX Firewall clusters, which safeguards the customer's users, applications, and infrastructure against advanced threats. These firewalls are fully equipped for advanced security services including intrusion, detection, and prevention (IDP). They also address Denial of Service (DoS) and Distributed Denial of Service (DDoS) protection services, which include protection against protocol and resource-based attacks.

For a nominal extra fee, we can also put the customer's environment behind a VMware NSX edge gateway to provide another layer of advanced threat protection.

Intrusion, Detection, and Prevention System

While many cloud providers require customers to stand up their own appliance and implement their own Intrusion Detection and Prevention System (IDPS), IV provides IDPS implementation and management as a standard part of the E.V.E. hosting infrastructure.

Our IDPS monitors all the traffic going in and out of the network. If it looks like a threat actor is trying to exploit a known vulnerability, the system will take a predefined series of actions, such as block, alert, log, etc.

IV's IDPS is designed to be extremely vigilant and aggressive, automatically blocking any activity that looks like a medium- or high-level attack with a low to medium possibility of being a false positive. If the IDPS is blocking any communication that the customer requires, we can exclude those IP addresses from their security protocol — a process known as whitelisting.

Security Information and Event Management

IV provides security information and event management (SIEM), which proactively collects event log data from across the entire cloud environment and analyzes that data to identify potentially malicious activity. This helps us respond to security threats before they disrupt business operations or increase compliance risk.

IV's staff of security experts continually monitors the SIEM to not only detect and respond to potential threats, but to identify vulnerabilities and improve E.V.E.'s security infrastructure to prevent future attacks. For example, our staff is constantly blacklisting IP addresses from threat actors to keep customers safe.

DoS and DDoS Protection

Denial of Service (DoS) attacks, in which threat actors flood the targeted host or network with traffic until it cannot respond or crashes, cause significant business disruption by preventing authorized users from gaining access. Volumetric Distributed Denial of Service (DDos) attacks, such as SYN, ICMP, and UDP flood attacks, are an even more serious threat vector. Typically launched using IoT bots, they flood the target host or network with data packets to consume bandwidth and resources — often increasing incoming traffic volume exponentially and completely overwhelming the system. IV's DDoS protection utilizes hundreds of nodes around the globe to filter out dangerous traffic to protect against these types of debilitating volumetric attacks.

Few cloud providers offer protection against both DoS and Volumetric DDoS attacks, and if they do, they charge you a significant fee for them. With IV, DoS and Volumetric DDoS are included in a customer's monthly hosting fee.

Multifactor Authentication

Multifactor Authentication (MFA) is a highly efficient way to verify a user's identity. It works by requiring users to confirm multiple factors before permitting access, instead of just relying on a username and password. Authentication factors can include something the user knows, such as a password; something they possess, like a security key or device; or something they are, such personal biometric data (fingerprint).

IV started offering MFA long before it became a common requirement for obtaining cyberinsurance. It is available to IV customers for a nominal monthly fee to provide further protection against malicious cyber-threats.

Data Encryption

IV enforces encryption between the desktop and the server for protocols such as remote desktop, SFTP, and HTTPS. We also encrypt all data that is replicated between our primary and secondary data centers to protect against access, modification, or theft.

For added protection, IV offers encryption at rest for data stored within E.V.E. for a nominal additional monthly charge. All stored data is encoded using encryption algorithms. Even if a malicious actor were to remove a hard drive from the E.V.E. data center (an act that would be prevented by physical building security), encryption at rest would prevent them from accessing any customer information on that drive.

Managed Detection and Response

IV Managed Detection & Response (MDR) provides AI-powered prevention, detection, response, and threat hunting across the customer's IV hosted servers and local user endpoints — all for a nominal extra charge.

IV offers two levels of MDR. Standard MDR leverages autonomous, AI-powered cybersecurity technology to deliver real-time threat hunting, prevention, detection, and response during normal business hours. Advanced MDR combines AI technology with human expertise to provide 24x7 threat hunting, monitoring, and response in real time. IV's Security Operations Center is staffed by threat intelligence analysts and security staff and utilizes detection forensics and risk alerts to protect customers against threats.

Patch Management

Patch management is essential to cybersecurity because it updates operating systems and closes security gaps that can leave businesses exposed. Because threat actors quickly uncover the vulnerabilities of each operating system, any business running an older (unpatched) version is potentially wide open to dangerous cyberattacks such as ransomware and malware.

That's why IV not only recommends that customers run current operating systems, but that they take advantage of our automated patch management service to automatically download the latest patches from vendors, ensuring that systems are updated regularly and known security vulnerabilities are fixed to minimize risk of attack.

Read-Only Backups

IV's backups are immutable, read-only snapshots taken by the NetApp storage controller within E.V.E., which means our approach doesn't rely on third-party software that could fail and prevent backups. These backups are not tied into the operating system or the active directories on the customer's server. As a result, threat actors cannot delete these backups — even if they were to login to the operating system on a virtual machine and take over the system

NetApp takes a perfect point-in-time snapshot instantaneously and replicates it block by block to the secondary data center storage system. As those blocks change, the changes are written elsewhere. When the next snapshot is taken, all the data that was created or modified since the last snapshot is frozen. In this way, the snapshots build upon each other to provide three months' worth of perfect crash-consistent backups.

For even greater security, IV goes one step further and runs an application-consistent backup every night. This coordinated, application-consistent snapshot ensures that IV can provide a completely clean and complete restore of your virtual machines at any given point in time — in only a matter of minutes — by mounting a read-only backup into a read-write volume and connecting the virtual machine to that volume. From the customer's perspective, it's like a simple system reboot.

Security Glossary

Intrusion Detection and Prevention System (IDPS): a system that monitors network traffic, scans for potential threats or policy violations, sends notifications to system administrators, and initiates automated actions to prevent possible incidents.

Denial of Service (DoS) attack: a cyberattack in which a threat actor seeks to render a machine or network resource unavailable to its intended users by disrupting a host or service connected to a network. This disruption is typically accomplished by flooding the targeted machine or resource with a huge volume of traffic to overload systems and prevent fulfillment of legitimate requests.

Distributed denial-of-service (DDoS) attack: a DoS cyberattack in which the incoming traffic flooding the target machine or resource originates from many different, or distributed, sources.

Encryption: A process that scrambles text into a format that cannot be read by malicious actors and requires that intended recipients use a decryption key to unscramble the text and make it readable.

Firewall: a security device that protects a network by blocking unwanted traffic or potentially malicious sources, thereby helping prevent unauthorized access to data.

Managed Detection & Response (MDR): a service that provides real-time threat hunting, monitoring, and response capabilities with autonomous protection and/or 24x7 threat notification and remediation managed by a team of security experts.

Multifactor Authentication (MFA): an electronic authentication method by which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence.

Patch management: the process of distributing and applying updates to software and devices in order to fix known bugs or vulnerabilities.

Read-only backup: a data backup in which files cannot be modified or deleted.

Security Information and Event Management (SIEM): a software solution that aggregates and analyzes activities from resources across your IT infrastructure. SIEM collects security data from network devices, servers, domain controllers, and other resources and runs them through analytic tools to identify threats, uncover trends, and deliver actionable insights to improve security.

SSAE 18 Type II Audit: an audit that evaluates a service organization's system, controls, and processes, including those related to cybersecurity, over a period of time (typically 3-12 months) to determine if they operated as intended.