Our Security, Your Victory

SecureVic is one of the leading professional services companies by providing world-class IT security services to clients from various industries, locally, regionally and internationally.

SECUREVIC

COMPANY PROFILE

CONTENT

ABOUT US

SecureVic is one of the leading professional services companies by providing world-class IT security services to clients from various industries, locally, regionally and internationally.

Our unique industry-based, consultative approach helps clients envision, build and reduce risk and provide operational efficiency.

We are committed to supply excellent quality IT products and complete solutions that include systems and storage, networking and security, virtualization and data protection, wireless as well as managed services.

Our success has been built on providing exceptional level of services to our customers. We pride ourselves on our responsiveness, agility and flexibility; in short to support customers' business objectives.

OUR PRODUCTS

arcserve

Check Point SOFTWARE TECHNOLOGIES LTD

CYBERARK

IMPERVA

ixia

Malwarebytes

paloalto NETWORKS

Proton Protect what you share

SECUREVIC

solarwinds

Symantec.

tenable

THALES

veeAM

WINMAGIC DATA SECURITY

ARCSERVE

Data availability delivered the way you need it

Not all data is created equal. Marketing brochures and file-sharing sites can typically withstand a few hours of downtime, while transactional systems are often mission-critical and must be available in seconds. Meanwhile, rising storage costs and strict compliance mandates demand affordable, long-term retention options.

Only Arcserve offers a full range of capabilities that allow you to cost-effectively apply the right level of data protection to your unique systems, and eliminate the need to layer on complex point solutions as business needs evolve.

Take control of your data protection

Today's availability needs require an innovative approach to data protection; one that allows you to achieve enterprise-grade protection without the complexity associated with enterprise solutions. Through one elegantly simple user console, you holistically configure and manage all aspects of your data protection strategy, from long-term storage to instant recovery, with complete control and visibility across all systems, applications and data.

Guarantee data availability with Arcserve UDP.
We've invested over five million development hours into redefining how businesses deploy and manage data protection with a single solution that delivers system resiliency across the entirety of your cloud, virtual, and physical systems.

High Availability - For critical data and applications that need to be accessible in seconds, our high availability technology delivers near-zero downtime from local, remote, or cloud-mirrored systems.

Disaster Recovery - DRaaS brings your systems back to life in minutes with ultra-efficient replication to a public or private cloud. Instantly run physical and virtual systems with full failover and failback capabilities, in an emergency or on an as-needed basis.

Backup & recovery - Our backup and recovery solution guarantees recovery with tape, disk, and cloud from virtual or on-premise data centers, public and private clouds, and remote geographical locations.

Email & archiving - Long-term email archiving delivers the searchable, granular archive you need for complete email compliance, regardless of whether you employ an on-premise or cloud-based email platform.

CHECK POINT INFINITY

Virtually all IT Security organizations seek to improve their ability to mitigate risk at a reasonable, sustainable investment level. Three challenges make this extremely difficult:

1. An aggressive, rapidly evolving threat landscape.

2. The organization's dynamic, evolving set of data, applications and infrastructure that need to be protected (mobile, cloud/SaaS, and third party outsourcing are but three examples).

3. Finding and retaining security staff that can translate business goals into technical strategies that are effective and sustainable over time.

Given these challenges, many in the industry have concluded that true protection is unattainable, and therefore the focus should move to detecting and mitigating threats after they have penetrated defences. This however is a very risky strategy. What is needed is a security architecture that adapts to dynamic business demands and is focused on prevention to ensure all key assets are completely protected.

Check Point Infinity is the only consolidated cyber-security architecture that future-proofs your business and IT infrastructure across all networks, cloud and mobile. Infinity leverages three key advantages to solve the challenges faced by IT Security:

1. Advanced Threat Prevention:

The industry's leading suite of protection capabilities, deployed across networks, cloud and mobile.

2. Threat Intelligence Platform:

The Check Point ThreatCloud, which amalgamates and distributes threat intelligence and protection updates in real-time.

3. Consolidated Management:

A unified management interface that allows business-oriented risk policies to be operationalized into security protections, with APIs for integration with IT infrastructure and applications.

Check Point Infinity provides complete protection from known and zero-day attacks across the environment, including cloud and mobile. The simple, business-oriented management interface reduces complexity, making it easier to deliver security and compliance with constrained staff and budget. Infinity helps organizations deliver agile yet secure IT, which can adapt as business requirements change. Through advanced threat revention, business-oriented policy management, and cloud-based threat intelligence, Infinity delivers a solid foundation for a sustainable, effective risk management strategy.

CYBERARK

PRIVILEGED ACCOUNT SECURITY SOLUTION

Know the Path of an Attack and Block it with Privileged Account Security

Privileged accounts represent the largest security vulnerability an organization faces today. These powerful accounts are used in nearly every cyber-attack, and they allow anyone who gains possession of them to control organization resources, disable security systems, and access vast amounts of sensitive data.

To protect these accounts and the critical resources they provide access to, organizations need comprehensive controls in place to protect, monitor, detect and respond to all privileged account activity.

CyberArk is the trusted expert in privileged account security. Designed from the ground up for security, the **CyberArk Privileged Account Security Solution** provides the most comprehensive solution for on-premises, cloud and ICS environments. This complete enterprise-ready Privileged Account Security Solution is tamper-resistant, scalable and built for complex distributed environments to provide the utmost protection from advanced external and insider threats.

Protect Credentials:

Organizations implement proactive controls that lock down privileged account passwords and SSH keys. By storing these credentials securely, restricting access to them, and automatically rotating them, organizations can reduce unauthorized use of privileged accounts.

Secure Sessions:

Organizations secure and control privileged sessions with session isolation. This creates separation between an administrator's endpoint and critical assets, ensuring that malware on a user's endpoint cannot spread to a target asset. Session isolation also prevents privileged credentials from ever being seen by the user or reaching and being stored on a potentially compromised endpoint.

Enforce Least Privilege and Endpoint Protection:

Organizations limit administrative and super-user rights on servers and endpoints to mitigate intentional and accidental misuse of excessive privileges. Least privilege enforcement enables organizations to reduce the attack surface while also enabling users to remain productive by easily requesting elevated privileges when necessary. Organizations may also secure endpoints by closely controlling and monitoring applications via whitelist, blacklist, and "greylist" (restricting unknown applications).

Continuous Monitoring:

Organizations implement continuous monitoring of all privileged account use, including live monitoring as well as behavioral analytics. Should an attacker manage to hijack a privileged account, continuous monitoring capabilities can help an organization detect the malicious behavior based on events or patterns of events that fall outside baselines generated specifically for the authorized user. Compromises can be addressed promptly by automatically rotating credentials or otherwise preventing continued unauthorized access to the affected privileged accounts.

IMPERVA

WEB APPLICATION SECURITY

Protect Your Critical Web Applications and Data

Web applications are a prime target of cyber attacks because they are readily accessible and offer an easy entry point to valuable data. To combat cyber attacks, organizations need to protect websites and applications from existing and emerging cyber threats without affecting application performance or uptime. More organizations rely on Imperva to protect their critical web applications than any virtual and cloud-based data centers, and deliver the market's most advanced web application security, constantly updated with threat intelligence curated by the renowned Imperva Application Defense Center research team.

Imperva SecureSphere Web Application Firewall

SecureSphere Web Application Firewall analyzes all user access to your businesscritical web applications and protects your applications and data from cyber attacks. SecureSphere Web Application Firewall dynamically learns your applications' "normal" behaviour and correlates this with the threat intelligence crowd-sourced from around the world and updated in real time to deliver superior protection. Imperva was recognized as the only leader in Gartner's Magic Quadrant for Web Application Firewalls. The industry-leading SecureSphere Web Application Firewall -looking website inclusion; business logic attacks such as site scraping and comment spam; botnet and DDoS attacks; and account takeover attempts in real-time, before fraud can be performed.

WEB APPLICATION SECURITY PRODUCTS

- **Web Application Firewall**
  Accurate, automated protection against online threats.
- **ThreatRadar Reputation Services**
  Leverage reputation data to stop malicious users and automated attacks.
- **ThreatRadar Community Defense**
  SecureSphere deployments around the world provide crowd-sourced threat intelligence to subscribers.
- **ThreatRadar Fraud Prevention**
  Stop fraud malware and account takeover quickly and easily.
- **Incapsula SaaS WAF and DDoS Protection**
  Best-of-breed web application security and content delivery as a service.

DATABASE SECURITY PRODUCTS

- **Database Activity Monitor**
  Full auditing and visibility into database data usage.
- **Database Firewall**
  Activity monitoring and real-time protection for critical databases.
- **Database Assessment**
  Vulnerability assessment, configuration management, and data classification for databases.
- **User Rights Management for Databases**
  Review and manage user access rights to sensitive databases.
- **ADC Insights**
  Pre-packaged reports and rules for SAP, Oracle EBS, and PeopleSoft compliance and security.

FILE SECURITY PRODUCTS

- **File Activity Monitor**
  Full auditing and visibility into file data usage.
- **File Firewall**
  Activity monitoring and protection for critical file data.
- **User Rights Management for Files**
  Review and manage user access rights to sensitive files.
- **Directory Services Monitor**
  Audit, alert, and report on changes made in Microsoft Active Directory.

IXIA

ixia

We provide testing, visibility, and security solutions to strengthen applications across physical and virtual networks.

Organizations use our tools and capabilities to test, secure and visualize their networks so their applications run stronger.

Product Offering Category:

Test:

- **Network Security Testing – BreakingPoint**
  Validate the security posture of your networks with real applications and complete range of threat vectors.
- **IxLoad**
  Measure the quality of experience of real-time, business-critical applications with converged multiplay service emulations.
- **Network Performance – IxNetwork**
  Validate the scale, performance and resilience of hyper-scale data centers.
- **IxChariot**
  Instantly assess performance of complex network infrastructures, including the public cloud.
- **IxANVL**
  Validate protocol compliance and interoperability.
- **IxVerify**
  Verify the performance of networking chips—from design to development.
  The industry's only solution purpose-built for 'pre-silicon' testing.
- **Ixia IoT - for IoT Device Testing**
  Characterize and optimize IoT devices under real-world deployment conditions.
- **IxVeriWave**
  Achieve high-performing WLAN Networks through comprehensive Wi-Fi testing.
- **IxLoad Wireless - LTE/4G Performance Testing**
  Test end-to-end performance of wireless LTE networks and components with emulation of multiplay services.
- **Developer - Debugging Tool**
  Helps developers find bugs early in the development cycle with agile application performance and security resilience test tool.
- **CloudShell**
  Complete lab automation and Lab-as-a-Service platform.

Network Security Tools:

- **Network Security Testing – BreakingPoint**
  Validate the security posture of your networks with real applications and complete range of threat vectors.
- **ThreatARMOR**
  Block known bad traffic to identify breaches faster.
- **AppStack**
  Advanced intelligence and application-level visibility.
- **Application and Threat Intelligence Subscription**
  Continuous real-time data feeds to ensure current application and threat intelligence at all times.

Malwarebytes

MALWAREBYTES

Malwarebytes offers two endpoint protection platforms featuring seven layers of technology, driven by the industry's best-informed telemetry, to protect your endpoints against known and unknown threats.

- Multi-Vector Protection
- Threat visibility dashboards
- Integrated remediation engine
- Centralized management

Ransomware Malware PUPs Adware Zero-day exploits

Malwarebytes anti-ransomware technology

Multi-Vector Protection - Malwarebytes Multi-Vector Protection technology reduces your exposure to ransomware and other advanced threats by blocking the different attack vectors used to distribute malicious code.

Block ransomware delivery - Malwarebytes Endpoint Protection prevents even the introduction of ransomware onto an endpoint by using proprietary anti-exploit technology that blocks a common means of ransomware delivery.

Prevent ransomware execution - Malwarebytes behavioral monitoring prevents ransomware from encrypting files by monitoring processes for malicious behavior and stopping the ransomware from executing its code.

Malwarebytes endpoint remediation

Respond quickly - Accelerate incident response workflows by deploying Malwarebytes Incident Response on your endpoints in advance, shortening the time between malware detection and removal.

Automate threat response - Schedule automated scans or leverage the non-persistent, dissolvable agent to automate the response to an incident alert.

Through endpoint remediation – Our proprietary Linking Engine removes the infection, including all related artifacts, returning the endpoint to a truly healthy state.

Malwarebytes technology complements antivirus

Strengthen traditional AV - Traditional AV solutions alone cannot protect against the advanced threats organizations face daily. Adding Malwarebytes Endpoint Protection ensures your endpoint, users, and data have the protection they need.

Multi-Vector Protection - Multi-Vector Protection provides a layered approach, including multiple signature-less techniques to protect against the threats traditional AV misses.

Integrated remediation capabilities – Our proprietary Linking Engine removes the infection, including all related artifacts, returning the endpoint to a truly healthy state.

Malwarebytes Endpoint Protection technology

Multi-Vector Protection - Multi-Vector Protection provides a layered approach, including multiple signature-less techniques, to protect against traditional viruses as well as tomorrow's attacks.

Integrated remediation capabilities – Our proprietary Linking Engine removes the infection, including all related artifacts, returning the endpoint to a truly healthy state.

Increase protection, reduce complexity - Malwarebytes Endpoint Protection's single endpoint agent combines powerful detection and remediation capabilities for better protection and faster response while reducing deployment and management complexity.

PALO ALTO NETWORKS

PALO ALTO NETWORKS Next-Generation Firewall

Fundamental shifts in the application and threat landscape, user behavior, and network infrastructure have steadily eroded the security that traditional port-based firewalls once provided. Your users are accessing all types of applications using a range of device types, often times to get their job done. Meanwhile, datacenter expansion, virtualization, mobility, and cloud-based initiatives are forcing you to re-think how to enable application access yet protect your network.

Traditional responses include an attempt to lock down all application traffic through an evergrowing list of point technologies in addition to the firewall, which may hinder your business; or allowing all applications, which is equally unacceptable due to increased business and security risks. The challenge that you face is that your traditional port-based firewall, even with bolt-on application blocking, does not provide an alternative to either approach. In order to strike a balance between allowing everything and denying everything, you need to safely enable applications by using business-relevant elements such as the application identity, who is using the application, and the type of content as key firewall security policy criteria.

Key safe enablement requirements:

Identify applications, not ports. Classify traffic, as soon as it hits the firewall, to determine the application identity, irrespective of protocol, encryption, or evasive tactic. Then use that identity as the basis for all security policies.

Tie application usage to user identity, not IP address, regardless of location or device. Employ user and group information from enterprise directories and other user stores to deploy consistent enablement policies for all your users, regardless of location or device.

Protest against all threats—both known and unknown. Prevent known vulnerability exploits, malware, spyware, malicious URLs while analyzing traffic for, and automatically delivering protection against highly targeted and previously unknown malware.

Simplify policy management. Safely enable applications and reduce administrative efforts with easy-to-use graphical tools, a unified policy editor, templates, and device groups.

Safe application enablement policies can help you improve your security posture, regardless of the deployment location. At the perimeter, you can reduce your threat footprint by blocking a wide range of unwanted applications and then inspecting the allowed applications for threats— both known and unknown. In the datacenter – traditional or virtualized, application enablement translates to ensuring only datacenter applications are in use by authorized users, protecting the content from threats and addressing security challenges introduced by the dynamic nature of the virtual infrastructure. Your enterprise branch offices and remote users can be protected by the same set of enablement policies deployed at the headquarters location, thereby ensuring policy consistency.

PROT-ON

Prot-On is an application that allows you to protect the files you share on the Internet and decide who, when and how can access them.

Share your files through any channel you want, by email, with a USB device, uploading to the cloud.

If you change your mind you can take away access to any of the protected copies wherever they are.

Protect Your File

Protect your file (PDF, Word, Excel, PPT...), texts, video files, audio files, images, AutoCAD, Photoshop files.

Control Access

Decide who, when and how (read, print, edit...) someone can access the protected files, wherever they are.

Track Document Use

At any time you can check the activity log to see who has been accessing any copy of your document.

SECURITY SYSTEMS

CCTV / Surveillance Systems – Commercial & Residential

We offer professional planning, installation, and maintenance for your security surveillance systems. You can always have an eye on your business & house whether you are at the office & house or if you are on vacation. Our services are performed with modern technology products. Your surveillance system will work even when you are off.

Alarm Security System & Monitoring – Commercial & Residential

We offer hard wired and wireless systems for your office building & house. We take care of your businesses & house security, so you can stay focused on your daily routine. We ensure your hard work will be protected at all times.

Door Access System - Commercial

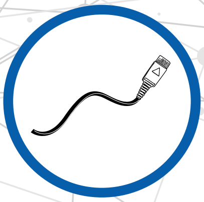
As technology improves, many companies are now issuing employee IDs capable of doing much more than simply identifying the cardholder. Employee ID badges can be integrated with access control systems for office buildings, restricted areas, and even company computers and networks. The badges can be activated and disabled as workers come and go to keep your office space secure and your computer systems/networks protected.

Fire Alarms - Commercial & Residential

We offer large, medium, and small commercial fire alarm systems that keep your business, occupants, and building protected. We create our systems to work all hours of the day so you don't have to worry about the alarm not working. We work with some of the largest corporations in the country–no building or business is too large or too small for us to ensure protection from a fire.

Auto Gate & Barrier Gate System

Gate systems services are normally hired to get the best level of protection and it is expected that it would protect people and their property and assets. We also provide the installation, upgrading and maintenance service for Auto gate & Barrier Gate system.



Structured Cabling Service

The cabling in your environment is the lifeblood, delivering users the speed and bandwidth needed to go to work. The right infrastructure is the key to a functional network. At SecureVic we provide a solid and scalable services over Network Cabling: Cat 5e, 6, Fibre Optic Cabling, Voice Cabling, Coax and Electrical Wiring.

SOLARWINDS

Network Management

Network Performance Monitor

Reduce network outages and improve performance with advanced network monitoring software.

Key Features:

- Multi-vendor network monitoring
- NetPath™ critical path visualization
- Performance analysis dashboard
- Intelligent alerts
- Network Insight for Cisco ASA
- Network Insight for F5 BIG-IP

Network Configuration Manager

Automated network configuration and compliance management.

Key Features:
- Network automation
- Network compliance
- Configuration backup
- Vulnerability assessment
- Network Insight for Cisco ASA
- Integration with Network Performance Monitor

IP Address Manager

Save time and prevent costly errors with affordable, easy-to-use IP address management software.

Key Features:
- Automated IP address tracking
- Integrated DHCP, DNS, and IP address management
- IP alerting, troubleshooting, and reporting
- Multi-vendor DHCP and DNS support
- Integration with VMware vRealize Orchestrator
- API Support

User Device Tracker

Locate users and devices on your network with User Device Tracker.

Key Features:
- Quickly locate network devices
- Map and monitor WAPs, switches, and ports
- Manage switch and switch port capacity
- Detect rogue devices and users
- Turn ports on and off remotely
- Unified IT administration dashboard

NetFlow Traffic Analyzer

Network traffic analyzer and bandwidth monitoring software.

Key Features:
- Bandwidth monitoring
- Network traffic analysis
- Performance Analysis Dashboard
- CBQoS policy optimization
- Customizable network traffic reports
- NBAR2 advanced application recognition

VoIP and Network Quality Manager

Deep dive into critical call QoS metrics and WAN performance insights.

Key Features:
- Monitor WAN QoS performance
- Troubleshoot VoIP call quality problems
- Cisco VoIP gateway and PRI trunk monitoring
- Visual VoIP call path trace
- Simplify IP SLA setup
- Optional High Availability

Engineer’s Toolset

Over 60 must-have network troubleshooting and diagnostic tools.

Key Features:
- Automated network discovery
- Real time monitoring and alerting
- Powerful diagnostic capabilities
- Enhanced network security
- Configuration & log management
- IP address and DHCP scope monitoring

Network Topology Mapper

Automatically plot your network in minutes with network mapping software.

Key Features:
- Automate device discovery and mapping
- Build multiple maps from a single scan
- Export network diagrams to Visio
- Auto-detect changes to network topology
- Perform multi-level network discovery
- Address regulatory PCI compliance

Kiwi CatTools

Powerful network automation and configuration management software.

Key Features:
- Schedule automated backups
- Perform bulk configuration changes
- Increase security
- Rollback network configuration
- Compare and analyze config changes
- Generate automated email reports

SYMANTEC

SECURE WEB GATEWAY

Know the Path of an Attack and Block it with Privileged Account Industry's Leading On-Premises Secure Web Gateway - Delivering advanced security for the web

Symantec Advanced Secure Gateway combines the functionality of the Symantec ProxySG secure web gateway with the intelligence of Symantec Content Analysis to offer a single, powerful web security solution that delivers world-class threat protection. Advanced Secure Gateway is a scalable proxy designed to secure your web communications and accelerate your business applications. The solution's unique proxy architecture allows it to effectively monitor, control, and secure traffic to ensure a safe web and cloud experience.

- Control web and cloud usage with fast app performance.
- Establish negative-day threat defense.
- Implement multi-authentication realm support.
- Gain visibility into encrypted web traffic.
- Achieve easy integration with advanced threat protection.

Advanced Real-Time Threat Protection - Gain complete protection and control

Add advanced threat protection to your secure web gateway with the Symantec Content Analysis system, featuring multiple antimalware engines, malware analysis (sandboxing), and endpoint integration. Symantec Intelligence Services and WebFilter offer real-time protection for web content, security categorization, web application control, and other capabilities as an optional subscription.

- Integrate real-time blocking of advanced threats.
- Deliver real-time sandboxing protection.
- Gain the most advanced web security.

Optimal secure web gateway proxy architecture - Strong security delivered the way you need it

Symantec secure web gateway solutions, including ProxySG, Advanced Secure Gateway, Secure Web Gateway Virtual, and Web Security Service, deliver strong proxy-based security in the form factor your organization needs: on-premises appliance, virtual appliance, in the cloud, or in a unified hybrid combination of these solutions. We bring together sophisticated technologies for mitigating risks and creating business advantages. As a core part of our secure web gateway platform, our proxy architecture—on-premises, in the cloud, and hybrid—will protect you against web- and network-based threats, enable cloud data protection, and give you flexible business policy control across the enterprise and the cloud, including web, social, and mobile networks.

- Gain full visibility and control for web and cloud access.
- Assess and control unsanctioned cloud usage.
- Combine security functions for cloud and mobile technologies.

World's Most Trusted Secure Web Gateway - Used by over 70% of Fortune Global 500

Our secure web gateway sits between your users and their interactions with the internet to identify malicious payloads and control sensitive content. The secure web gateway consolidates a broad feature set to authenticate users, filter web traffic, identify cloud application usage, provide data loss prevention, deliver threat prevention, and ensure visibility into encrypted traffic. It also provides coaching and feedback to ensure a strong and secure user experience on the internet. Further, it delivers consolidated policy management and reporting when you use it with our cloud-delivered secure web gateway, as a hybrid delivery model.

Backed by our real-time WebPulse Collaborative Defense technology, with the Negative Day Defense feature, your secure web gateway deployment is protected. Our cloud-based Global Intelligence Network features web and threat intelligence gained through our partnership with more than 15,000 of the largest global enterprises.

- Work seamlessly with top technologies.
- Get visibility into HTTPS or SSL-encrypted web traffic.
- Enjoy unmatched performance and reliability.

– TENABLE NETWORK SECURITY

Nessus Professional Vulnerability Scanner

Nessus is deployed by millions of users worldwide to identify vulnerabilities, policy-violating configurations and malware that attackers use to penetrate your or your customer's network.

23,000 organizations can't be wrong.

With Vulnerabilities, Seeing is Believing

Whether it's your IT environment or your customers, it's vulnerable – increasingly so! Digitization and the ever-extending enterprise propel this. But most organizations lack visibility – leaving blind spots for attackers. To be effective, you need one solution that lets you keep pace and see it all.

Get The Power of NESSUS Behind You

Nessus® Professional is the industry's most widely deployed assessment solution for identifying the vulnerabilities, configuration issues, and malware that attackers use to penetrate your, or your customer's network. With the broadest coverage, the latest intelligence, rapid updates, and an easy-to-use interface, Nessus offers an effective and comprehensive vulnerability scanning package for one low cost.

Key Features:

- Easy to Use - Policy creation is simple and only requires a few clicks to scan an entire network.
- Comprehensive Detection - The Nessus scanner covers more technologies and identifies more vulnerabilities, providing a higher detection rate than competing solutions.
- Low Total Cost of Ownership (TCO) - Complete vulnerability scanning solution with unlimited scans against unlimited IPs for one low cost.
- Fast & Accurate - High-speed accurate scanning with low false positives lets you quickly identify those vulnerabilities that need fixing first.
- Timely Protection - Tenable researchers leverage extensive intelligence sources – providing plug-ins that deliver timely response for the latest vulnerabilities and threats.
- Accommodate Growth - Easily move to Tenable.io – with tools that speed migration – as vulnerability management needs increase.

THALES

Data Encryption

Encrypt Everything, Everywhere

One data security solution for securing sensitive data across servers spanning your data centers, clouds, big data and container environments.

Operational Simplicity

Centralized policy and key management to assure control of your data across every physical and virtual server on and off your premises.

Minimize Risk

Meet compliance and best practice requirements for protecting data from external threats or malicious insiders with proven, high-performance and scalable data encryption.

Security Agility

Quickly address new data security requirements and compliance mandates by having a data encryption solution in place ready and able to encrypt everything.

Data Encryption Products

- Vormetric Data Security Platform
- Vormetric Data Security Manager
- Vormetric Transparent Encryption
- Live Data Transformation Extension
- Vormetric Container Security
- Vormetric Transparent Encrpytion for SAP HANA
- Security Intelligence Logs
- Vormetric Application Encrpytion
- Vormetric Cloud Encryption Gateway
- Vormetric Protection for Teradata Database
- Vormetric Orchestrator

veeaM

VEEAM

BACKUP & REPLICATION

Availability for the Always-On Enterprise

Veeam® Backup & Replication™ delivers Availability for ALL workloads — virtual, physical, and cloud — from a single management console, extending Veeam's leadership position from being the best for VMware vSphere and Microsoft Hyper-V to #1 Availability for any app, any data on any cloud. It allows customers to completely get rid of legacy backup forever and brings backup and replication together into a single software solution.

Veeam Backup & Replication Features

Backup

Veeam provides fast and reliable backup for virtual, physical and cloud-based workloads:

- Built-in management for Veeam Agent for Microsoft Windows and Veeam Agent for Linux : Get reduced data protection management complexity and improved usability through the addition of agent-based backup capabilities in the Veeam Backup & Replication consoleNEW, including a single pane of glass for Availability of virtual, physical and cloud workloads, centralized backup agent deployment, and Windows Server Failover Cluster support.
- Image-level VM backups: Create application-consistent backups with advanced application-aware processing.
- Backup from Storage Snapshots for Cisco, Dell EMC, Hewlett Packard Enterprise (HPE), IBMNEW, LenovoNEW, NetApp and Nimble: Generate ultra-fast backups with low RPOs.
- Scale-out Backup Repository™: Create a single virtual pool of backup storage to which backups can be assigned, offering the freedom to easily extend backup storage capacity.
- Veeam Cloud Connect: Get backups off site without the cost and complexity of building and maintaining an off-site infrastructure; fast and secure cloud backup to a service provider.
- SureBackup®: Automatically test and verify every backup and every virtual machine (VM) for recoverability.
- Built-in WAN acceleration: Get backups off site up to 50x faster and save bandwidth.
- Direct Storage Access: Perform vSphere backups faster and with reduced impact by backing up via Direct SAN Access and Direct NFS Access.

Recovery

Veeam delivers lightning-fast, reliable restore for individual files, entire VMs and application items — ensuring you have confidence in virtually every recovery scenario:

- Instant VM Recovery®: Recover a failed VM in less than two minutes.
- Instant File-Level Recovery: Recover guest OS files and folders on the fly.
- Veeam Explorer™ for Microsoft Active Directory: Instantly recover individual AD objects and entire containers, easily recover user accounts and passwords, enable restores of Group Policy Objects (GPOs), Active Directory- integrated DNS records and more.
- Veeam Explorer for Microsoft Exchange: Instant visibility and granular recovery of individual Exchange items, including hard-deleted items, detailed export reports for eDiscovery and more.
- Veeam Explorer for Microsoft SharePoint: Instant visibility into SharePoint backups; easily find and recover specific SharePoint items as well as individual sites.
- Veeam Explorer for Microsoft SQL Server: Fast transaction and table-level recovery of SQL databases allowing for precise point-in-time restore.
- Veeam Explorer for Oracle: Transaction-level recovery of Oracle databases, including agentless transaction log backups, enabling precise point-in-time restore.
- Veeam Explorer for Storage Snapshots: Recover single files and entire VMs from Dell EMC, HPE, IBMNEW, LenovoNEW, NetApp, and Nimble storage snapshots.
- Native tape support: Store entire VM backups or individual files on tape including features like direct restore from tape for growing enterprise environments.

WINMAGIC DATA SECURITY

SecureDoc™ for Windows Enterprise Edition

The Leading Innovator in Full-Disk Encryption

WinMagic provides intelligent key management for everything encryption, with robust, manageable and easy-to-use data security solutions. WinMagic's SecureDoc secures data wherever it is stored, providing enterprise grade data encryption and key management policies across all operating systems. WinMagic's SecureDoc Enterprise Edition maintains end user productivity while ensuring maximum security and transparency in regular work flow. Whether it's SecureDoc's software encryption, or Microsoft's BitLocker or easily integrating with industry-standard technologies such as OPAL-compliant Self-Encrypting Drives (SEDs), SecureDoc allows businesses to deal with the security of their IT environment efficiently. SecureDoc is trusted by thousands of enterprises and government organizations worldwide to minimize business risks, meet privacy and regulatory compliance requirements, while protecting valuable information assets against unauthorized access.

Additional features available SecureDoc Enterprise Edition include; PBConnex, Removable Media Container Encryption (RMCE) and File and Folder Encryption (FFE).

SecureDoc Enterprise for Windows Advantages:

Reduce TCO with PBConnex - less time spent on labor-intensive tasks (Password resets, Device Staging etc.)

- Opal SED Support – manage hardware encrypting drives in mixed environments.
- Supports all version of Windows – Win 10, Win 8, Win 7, Vista, XP.
- BitLocker Management with PBConnex support.

Features at a Glance:

- Only full-disk encryption solution to offer wired and wireless pre-boot network authentication via PBConnex.
- File & Folder Encryption.
- Removable Media Encryption.
- Removable Media Container Encryption.
- FIPS 140-2 validated.
- Support for:
  * Opal 1 and 2 Self-encrypting drives.
  * BitLocker – seamlessly manage BitLocker with SES and enhance security with PBConnex.

Our Security,
Your Victory

SECUREVIC

Securevic Sdn. Bhd. (1244799-D)

L, 16-05 PJX-HM Shah Tower, 16A Jalan Persiaran Barat, 46050 Petaling Jaya, Selangor Darul Ehsan, MALAYSIA.

Tel : +603-7931 9471 | Fax : +603-7931 8471 | Email : sales@securevic.my