HUGHES®

An EchoStar Company

Protecting Endpoints and Applications with Hughes

Introduction

There is a security gap in the coverage of many modern enterprises when it comes to prevention. Intrusion detection has come a long way over the years, but cybercriminals are constantly coming up with new ways to infiltrate networks. When these new attacks or exploits are found, they are known as zero-day threats or attacks. Intrusion detection systems can often miss them, and they are unable to consistently prevent threat actors from using zero-days to access your network. Security vendors need time to develop patches or hotfixes to stop the zero-days from spreading and being used in other places, but this takes days or even weeks to do.

Hughes Managed Cybersecurity takes a different approach. By leveraging deep learning, Hughes provides a prevention-first security model that stops cyber threats before they can execute. Unlike traditional solutions that rely on signatures, behavioral analysis, or cloud-based lookups, Hughes technology predicts and prevents threats in milliseconds, delivering industry-leading efficacy with minimal false positives.

Hughes Ransomware and Zero-Day Prevention is a lightweight agent that can be downloaded onto endpoints. It scans files and applications, ensuring their safety before the end user has a chance to interact with them.

The average cost of a data breach is now over $4.88M per incident, as of 2024.

Source: Cost of a data breach 2024 | IBM

Chapter 1: The Hughes Approach to Preventing Ransomware and Zero-Day Threats

A Prevention-First Approach

Unlike traditional security solutions that focus on detection, Hughes prioritizes true prevention. Many competing solutions rely on recognizing attack behaviors after a threat has already infiltrated an environment, which increases dwell time and the potential for damage. Hughes, however, leverages deep learning-driven artificial intelligence (AI) to prevent malware, ransomware, and zero-day threats before they ever execute, reducing the need for extensive post-attack remediation.

Superior Threat Efficacy and Accuracy

Threat efficacy is one of the most critical aspects of any cybersecurity solution. Many competitors struggle to maintain high accuracy against unknown malware, often producing false positives that drain security teams' time and resources. Hughes provides industry-leading accuracy, preventing more than 99% of known and unknown threats with a false positive rate of less than 0.1%. This means fewer false alarms and more efficient security operations.

Enhancing SOC Efficiency

Many cybersecurity solutions generate excessive amounts of telemetry data, overwhelming Security Operations Centers (SOCs) with alerts and requiring significant effort to triage and investigate threats. Hughes takes a more streamlined approach by preventing threats at the pre-execution stage. This reduces the overall data that SOC teams need to analyze, allowing them to focus on legitimate threats and accelerate response times.

Proactive AI for Unparalleled Protection

While many solutions rely on machine learning (ML) models that require constant updates, cloud lookups, and threat intelligence feeds, Hughes utilizes deep learning-based AI that autonomously prevents threats without relying on external data. This makes it more resistant to attacker evasion techniques and ensures real-time protection without the latency associated with cloud-dependent solutions.

True Ransomware Prevention

Most cybersecurity platforms detect ransomware only after it begins executing, often requiring rollback or remediation tools to recover encrypted data. However, rollback features can be unreliable, as they often depend on system backups that attackers can easily delete. Hughes eliminates this risk entirely by preventing ransomware from executing in the first place, ensuring that businesses never face the consequences of encryption or data exfiltration.

Consistent Protection Online and Offline

Many modern security solutions experience a sharp decline in efficacy when offline, as they rely on cloud-based engines to process threats. Hughes delivers equal levels of protection whether a device is online or offline, ensuring that endpoints remain secure regardless of connectivity status.

Ransomware payments surpassed a total of $1B in 2023, the highest ever recorded.

Source: https://www.chainalysis.com/blog/ransomware-2024/

Chapter 2: Protecting Endpoints

Cyber adversaries operate at an alarming pace, leveraging sophisticated techniques to bypass traditional security measures. Ransomware and zero-day threats present some of the most challenging risks to businesses today. Many security solutions struggle to keep up, often requiring minutes, hours, or even days to detect and respond to a threat—by which time, the damage has already been done. Hughes Managed Cybersecurity, leveraging Deep Instinct's advanced deep learning technology, is designed to stop these threats before they can execute, providing unparalleled protection for businesses of all sizes.

Stopping Threats Before They Attack

Traditional security tools, including legacy antivirus and behavior-based detection systems, rely on identifying attack patterns after they have begun executing. This reactive model leaves organizations vulnerable, as ransomware can begin encrypting files within seconds. Hughes eliminates this risk entirely by predicting and preventing ransomware, zero-day exploits, and malware before they have the opportunity to cause harm. With threat prevention occurring in less than 20 milliseconds, Hughes provides businesses with a critical layer of security that outpaces attackers.

AI-Powered Zero-Day Prevention

Zero-day attacks exploit previously unknown vulnerabilities, making them some of the most dangerous threats in cybersecurity. The Hughes deep learning-powered solution anticipates and blocks these attacks without relying on cloud lookups, signatures, or heuristic-based detection. This approach not only improves accuracy but also ensures that endpoints remain secure even when offline.

Seamless Integration and Automation

The Hughes prevention-first approach seamlessly integrates with existing security infrastructures, including Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and Endpoint Detection and Response (EDR) platforms. Automated responses allow for quick isolation, remediation, and threat intelligence sharing, streamlining security operations and reducing manual intervention.

Chapter 3: Protecting Applications

Eliminating Hidden Malware Before It Executes

Many security solutions focus on endpoints but overlook the files in transit—those uploaded, downloaded, or stored within an organization. Attackers take advantage of this blind spot, embedding malicious payloads in seemingly legitimate files. If these files are not properly scanned, they remain hidden until an unsuspecting user opens them, triggering an infection.

Hughes ensures these threats never get the chance to execute. With deep learning-based prevention, files are scanned in under 20 milliseconds, identifying and blocking malware before it can reach critical systems. This approach eliminates the need for reactive security measures that rely on detecting threats after they have already infiltrated the network.

Enterprise-Scale Protection with Minimal Latency

Organizations process millions of files daily, from customer uploads to internal document sharing. Traditional scanning solutions, such as sandboxes and antivirus engines, often struggle with scalability and introduce delays that disrupt user experience. Hughes overcomes these limitations by offering high-speed scanning that scales effortlessly to tens of millions of files per day.

By integrating seamlessly with web applications and cloud storage, Hughes provides real-time protection without impacting performance or user productivity. Whether scanning a single document or processing vast amounts of data, Hughes delivers the same level of accuracy and speed.

Protecting Applications from File-Based Attacks

Web applications, cloud services, and enterprise storage are primary targets for cybercriminals who exploit file uploads to deliver malware. Many security tools fail to effectively analyze these files, either due to inefficiencies in their scanning methods or an over-reliance on signature-based detection.

Hughes employs a deep learning-powered scanning engine that examines the full content of each file, not just its extension or metadata. This ensures that even the most well-disguised threats, such as obfuscated scripts or embedded ransomware, are accurately identified and blocked. Supported file types include:

- Executables (.exe, .dll, .sys)
- Office documents (.docx, .xlsx, .pptx)
- PDFs, archives (.zip, .rar, .tar)
- Scripts and macros embedded in documents
- Rich media files, including Java archives and font files

With comprehensive coverage across a wide range of formats, Hughes effectively prevents malware from slipping through unnoticed.

Hughes employs a deep learning-powered scanning engine that examines the full content of each file, not just its extension or metadata.

Seamless Integration with Existing Security Infrastructure

The Hughes solution is designed for flexibility, integrating effortlessly with existing security environments. Using REST API and ICAP protocol, Hughes can deploy across web gateways, firewalls, Cloud Access Security Broker (CASB) solutions, and cloud storage environments. This means organizations can enhance their security posture without overhauling their existing infrastructure.

Additionally, Hughes integrates with SIEM and SOAR platforms, providing valuable threat intelligence and automating responses to potential threats.

Chapter 4: How Hughes Uses Deep Learning to Stay Ahead of Cybercriminals

Cybercriminals are constantly changing their tactics. They are leveraging automation and AI, and constantly probe businesses for common weaknesses or mistakes they know they can take advantage of. The speed and complexity of modern attacks mean that organizations can no longer rely on outdated detection-based defenses. Instead, a prevention-first approach is necessary. It is much harder to secure your network if you allow cybercriminals easy access and rely too much on the ability to find and detect them. It is much more efficient if you can prevent them from ever getting into your network.

Beyond Traditional Security: The Shift to Deep Learning

Most cybersecurity solutions rely on ML, signature-based detection, or behavior analysis to identify threats. While these methods have been useful in the past, they have significant limitations:

- **Signature-Based:** Requires constant updates and only detects known threats. Completely ineffective against zero-day attacks
- **Behavior-Based Detection (EDR/NDR/XDR):** Detects threats only after execution has started, meaning attackers still gain initial access
- **Machine Learning:** While better than signature-based approaches, ML still requires frequent updates, relies on human-fed training data, and struggles against novel threats

Deep learning, on the other hand, is modeled after the way the human brain processes information. Unlike ML, which requires continual human intervention and retraining, deep learning autonomously identifies patterns in massive amounts of data, allowing it to predict and stop even never-before-seen threats with unmatched accuracy.

How Deep Learning Powers Prevention

The deep learning engine has been trained on billions of data points to recognize malicious code at an unprecedented speed and accuracy level. This enables Hughes to:

1. Prevent Ransomware, Zero-Days, and Unknown Malware in Milliseconds

- Hughes stops threats **pre-execution**, preventing malware from ever running—unlike detection-based solutions that allow threats to activate before responding
- It scans and classifies threats in **less than 20 milliseconds**, blocking ransomware faster than it can encrypt a single file
- With >**99% efficacy** against known and unknown malware, Hughes provides the strongest possible defense against emerging threats

2. Reduce False Positives to Increase SOC Efficiency

- Many security tools overwhelm security teams with false positives, wasting time and resources on investigating benign alerts
- Hughes has an industry-leading false positive rate of less than 0.1%, dramatically reducing alert fatigue and enabling SOC teams to focus on real threats

3. Predict and Block Evasive, AI-Powered Attacks

- Cybercriminals now use AI to craft polymorphic malware that constantly changes its signature to evade traditional detection
- The deep learning engine is designed to identify hidden malicious intent, blocking sophisticated AI-generated attacks that traditional security tools miss

Deep Learning vs. Machine Learning: Why Hughes Stands Apart

Many cybersecurity vendors claim to use AI, but not all AI is created equal. Traditional ML models have major weaknesses compared to the Hughes deep learning approach:

	Machine Learning	Hughes Deep Learning
Threat Recognition	Relies on pre-labeled datasets, requiring constant updates	Learns autonomously from raw data, detecting even unknown threats
Accuracy Over Time	Degrades as new threats emerge, requiring retraining	Continually improves, maintaining high efficacy against new malware
Processing Speed	Can take seconds or minutes to analyze threats	Stops malware pre-execution in <20 ms
Cloud Dependency	Often relies on cloud lookups for analysis	Fully on-device, providing protection even when offline
False Positives	Higher rate due to incomplete threat context	<0.1% false positives, reducing SOC workload

Chapter 5: The Cost of a Cyberattack. Why Prevention is the Best Investment

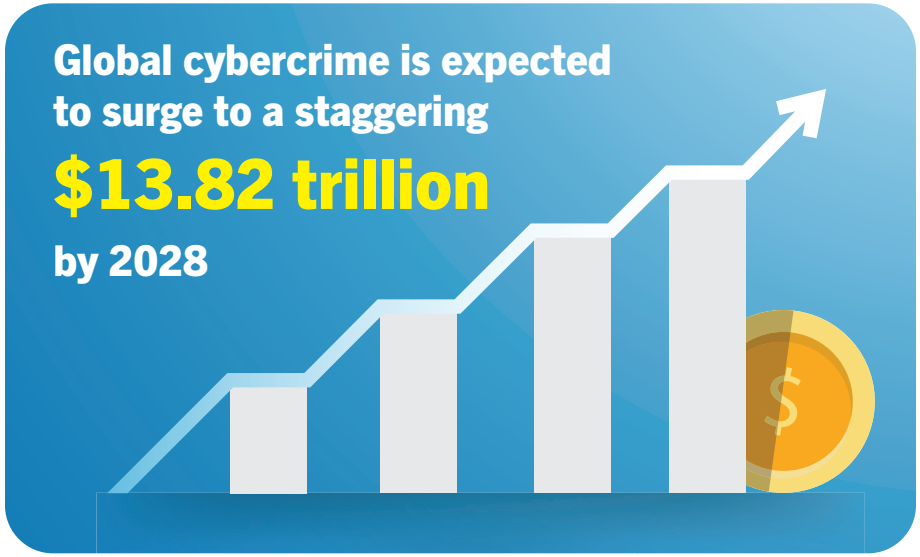
Cyberattacks are no longer rare, isolated events—they have become a daily reality for businesses of all sizes and industries. From ransomware crippling entire organizations to data breaches exposing millions of records, the financial and operational consequences of a successful attack can be devastating.

Yet, many companies still invest heavily in reactive security measures that only detect and respond to threats after they have already infiltrated the network. The problem? By the time a threat is detected, the damage is already done.

Hughes takes a different approach, offering prevention-first security that stops cyberattacks before they can execute—saving organizations from financial loss, downtime, reputational damage, and compliance penalties.

The Rising Cost of Cybercrime

Cybercrime is a booming industry, costing businesses trillions of dollars annually. According to recent reports:



Source: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

These numbers are intimidating, but the true cost of an attack goes beyond the immediate financial loss. Let's break down the key areas where organizations suffer after a successful cyberattack.

1. Ransom Payments and Recovery Costs

Ransomware has become one of the most financially damaging forms of cybercrime. Attackers encrypt critical files and demand a ransom—often in the millions—to restore access. However, paying the ransom does not always guarantee full recovery, and many organizations find themselves:

- Paying the ransom AND still needing expensive forensic investigations
- Facing weeks or months of downtime while restoring systems
- Dealing with repeat attacks, as paying the ransom marks them as an easy target

Hughes eliminates this risk by preventing ransomware from executing in the first place, meaning businesses never have to make the impossible choice between paying cybercriminals or losing critical data.

2. Business Downtime and Lost Revenue

A cyberattack does not just drain IT budgets—it disrupts entire business operations. Consider the following:

A ransomware attack takes an average of 21 days to recover from.

Source: https://www.cigent.com/blog/ransomware-and-recovery-time-what-you-should-expect

The longer a company is offline, the more revenue it loses. Every hour of downtime adds to the financial damage. Hughes ensures business continuity by stopping attacks before they start, keeping organizations running smoothly and avoiding costly disruptions.

3. Compliance Fines and Legal Consequences

Cyberattacks often expose sensitive customer and company data, triggering regulatory penalties under laws like:

- **General Data Protection Regulation (GDPR):** Fines up to €20 million or 4% of annual revenue for data breaches
- **California Consumer Privacy Act (CCPA):** Severe penalties for companies failing to protect consumer data
- **Health Insurance Portability and Accountability Act (HIPAA):** Costly fines for healthcare data breaches

Beyond fines, businesses can also face class-action lawsuits from customers whose personal information was exposed. Hughes prevents data breaches by blocking malware before it can access sensitive files, keeping organizations in compliance and avoiding financial penalties.

4. Reputational Damage and Customer Loss

Cyberattacks do not just impact financials—they erode customer trust. A high-profile breach can permanently damage a company's reputation:

- 60% of small businesses close within six months of a cyberattack due to lost customer confidence.
- 66% of customers say they would stop doing business with a company after a data breach.
- Stock prices of publicly traded companies drop down to 4% on average within a month of a cyberattack.

Rebuilding trust after a breach is difficult and expensive. The best way to protect brand reputation is to prevent cyber incidents from happening in the first place—a core strength of the Hughes prevention-first security approach.

Hughes Delivers Cost-Saving Benefits:

- **Eliminates Ransomware Risk:** No ransom payments, no data loss, and no downtime
- **Reduces False Positives:** Saves SOC teams time and lowers operational costs
- **Prevents Downtime:** Keeps businesses running, protecting revenue streams
- **Avoids Regulatory Fines**: Stops breaches before they happen, ensuring compliance
- **Protects Brand Reputation:** Customers trust companies with strong cybersecurity

Conclusion and Key Takeaways

In cybersecurity, the saying holds true: An ounce of prevention is worth a pound of cure. Hughes Ransomware and Zero-Day Prevention stops ransomware and zero-day threats better than any other intrusion detection platforms available on the market today. While detection and response tools are still very beneficial to have in place, it does not make sense for businesses to rely too heavily on the ability to detect threats when they could be preventing them altogether.

The Bottom Line: Prevention Saves Money

Organizations must shift their mindset from an overreliance on detection and response to a more balanced approach that leverages modern prevention and protection. The cost of one cyberattack can far exceed the investment in a prevention-first security solution like Hughes.

With Hughes, businesses gain peace of mind knowing they are protected from ransomware, zero-day threats, and unknown malware—saving millions in potential losses, while strengthening long-term security resilience.

Learn more about Hughes Managed Cybersecurity solutions:

www.hughes.com/what-we-offer/managed-cybersecurity

www.hughes.com/what-we-offer/managed-cybersecurity/ransomware-zero-day-prevention

HUGHES
An EchoStar Company

11717 Exploration Lane Germantown, MD 20876 USA
www.hughes.com

H72597 MAR 25